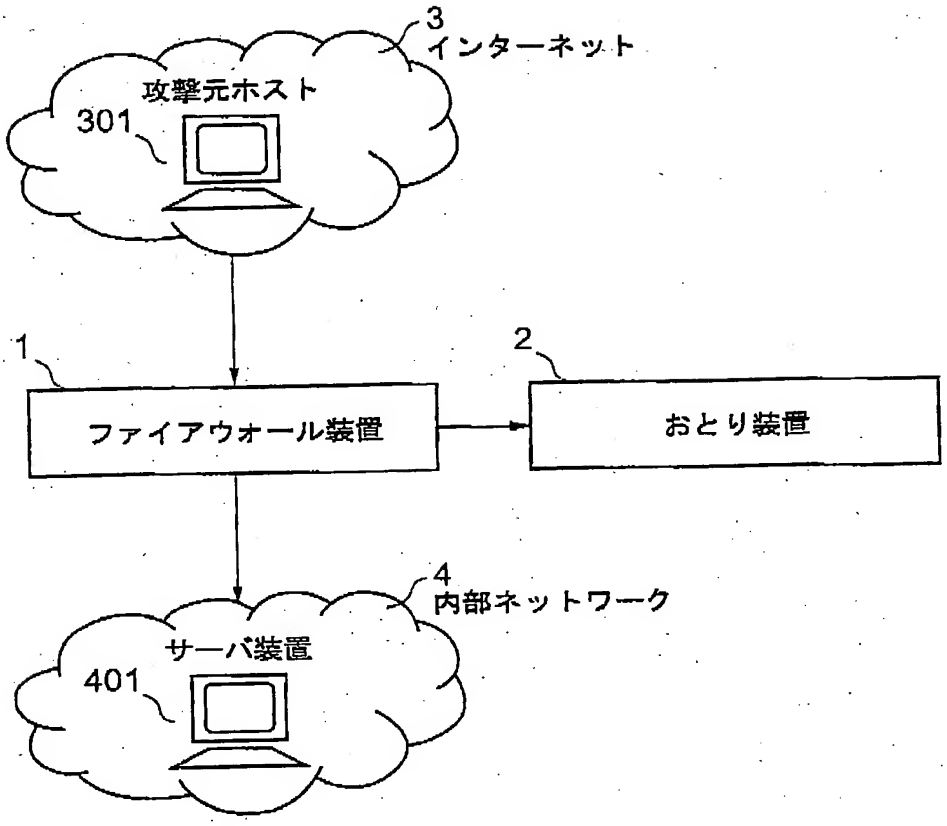
FQ5-613 0537

整理番号 0489

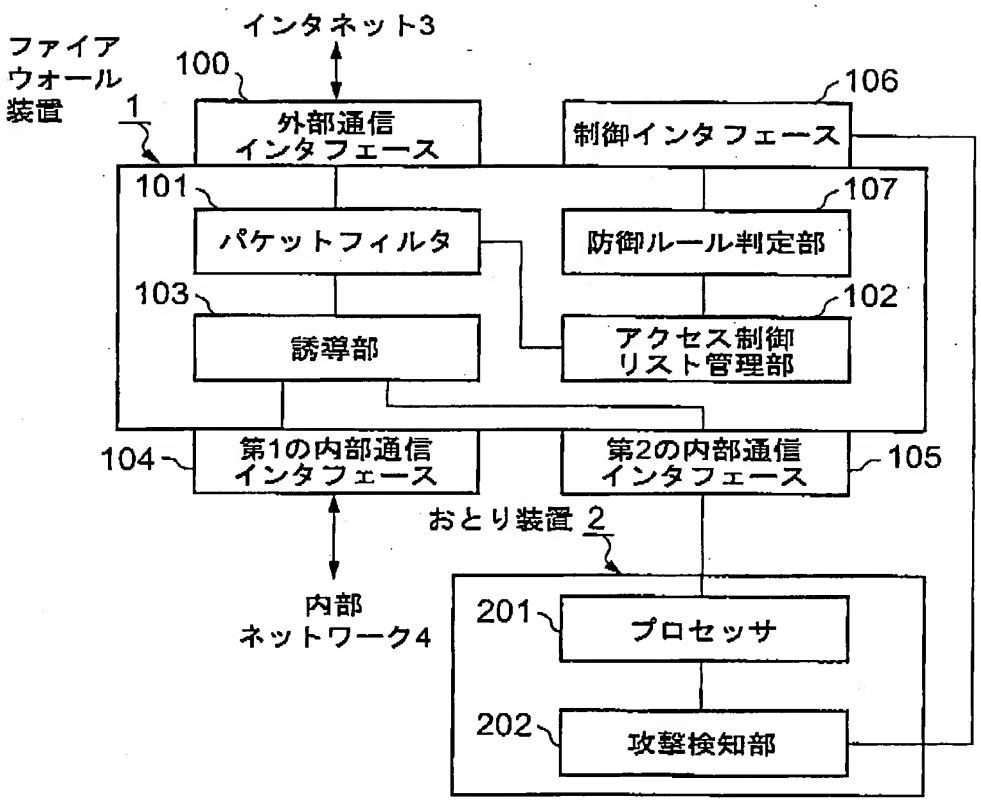
(1/31)

【書類名】　図面

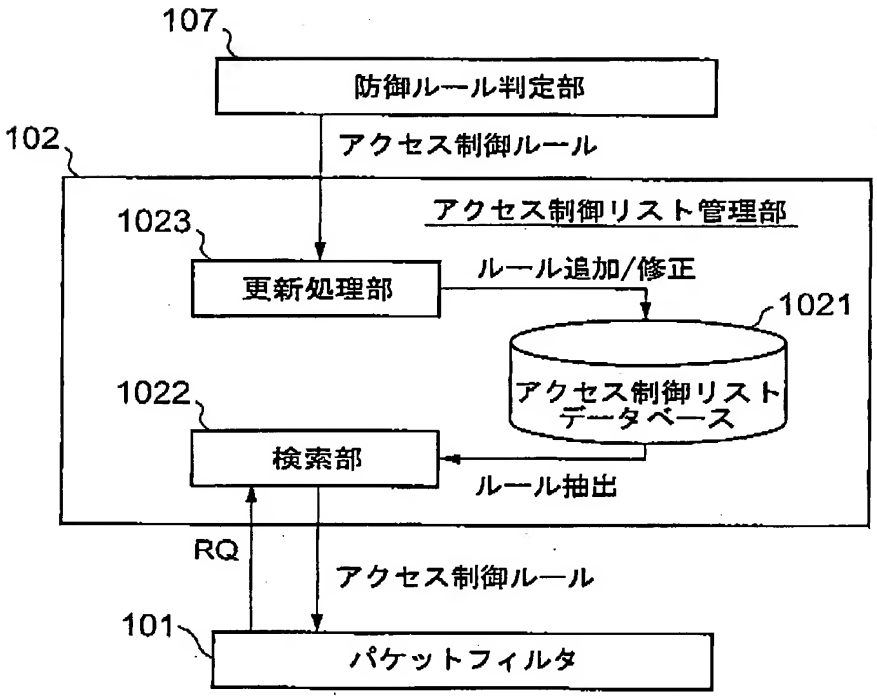
【図 1】



【図 2】


インタネット3
ファイア
ウォール
装置
1
100
外部通信
インタフェース
106
制御インタフェース
101
パケットフィルタ
107
防御ルール判定部
103
誘導部
102
アクセス制御
リスト管理部
104
第1の内部通信
インタフェース
第2の内部通信
インタフェース
105
おとり装置 2
内部
ネットワーク4
201
プロセッサ
202
攻撃検知部

【図 3】


107
防御ルール判定部
102
アクセス制御ルール
アクセス制御リスト管理部
1023
更新処理部
ルール追加/修正
1021
アクセス制御リスト
データベース
1022
検索部
ルール抽出
RQ
アクセス制御ルール
101
パケットフィルタ

【図 4】

1021

アクセス制御リストデータベース

ソースIPアドレス (SRC)	ディスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

*…任意のアドレスにマッチ
ACCEPT…パケットの受理
DENY…パケットの拒否(ICMPエラーを通知)
DROP…パケットの廃棄(ICMPエラーを通知しない)

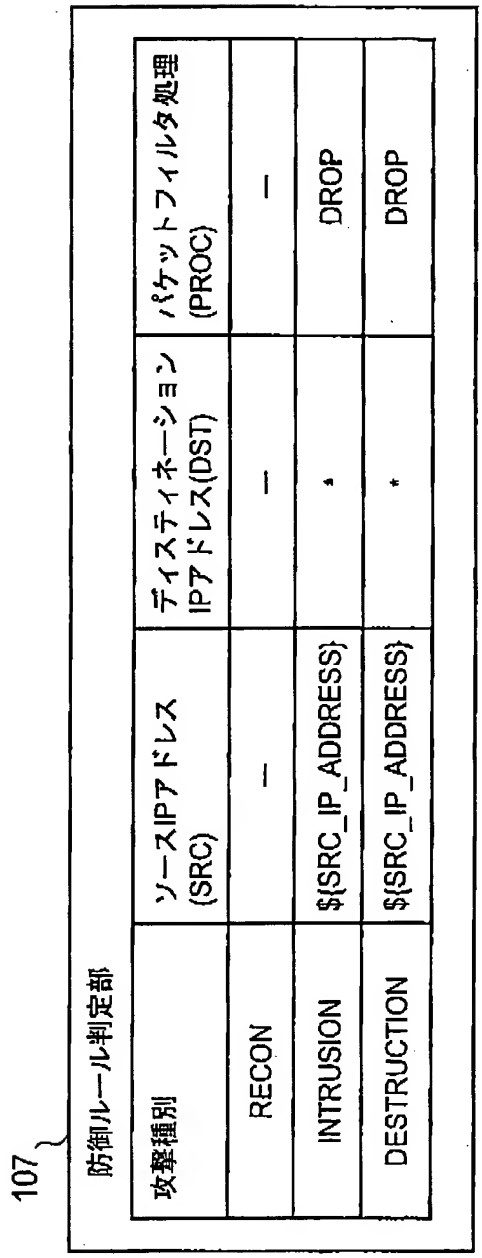
【図 5】

誘導リスト

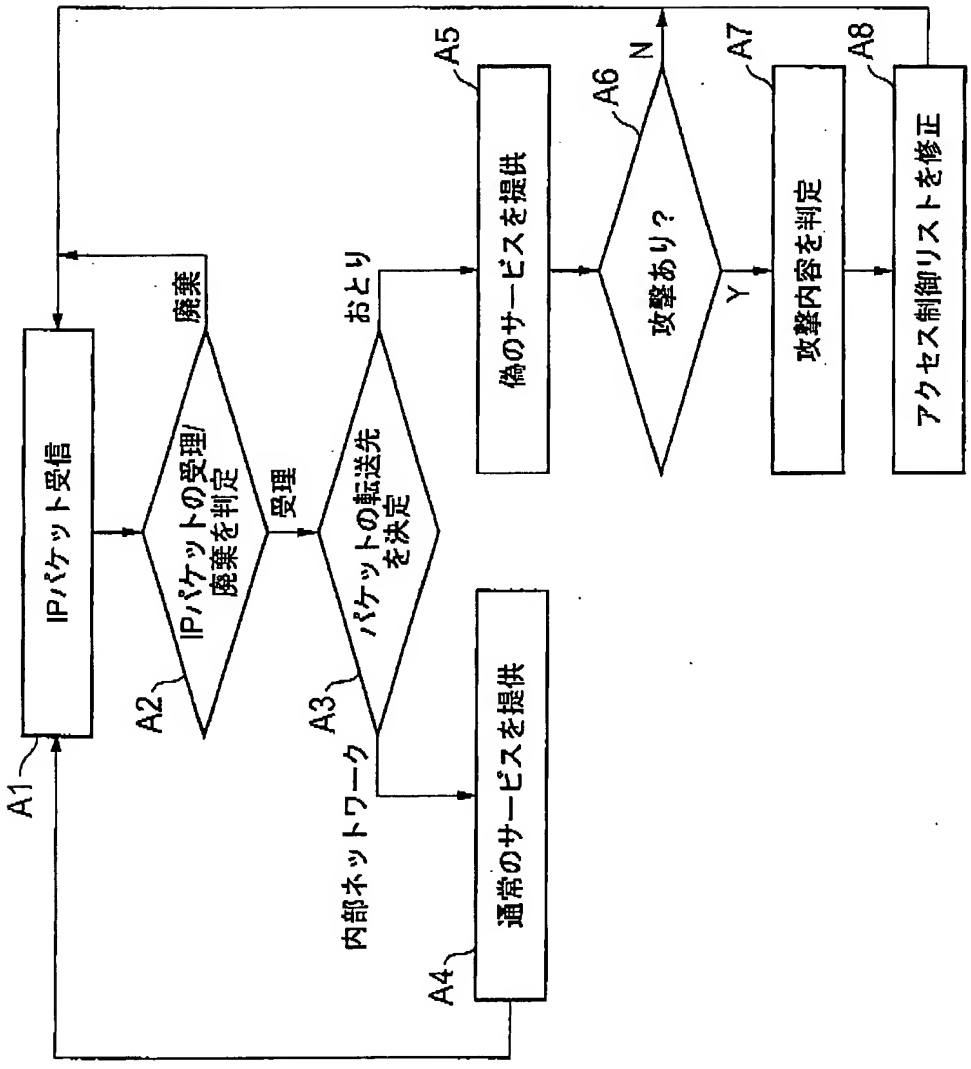
1. 2. 3. 1
1. 2. 3. 2
1. 2. 3. 3

1. 2. 3. 5
1. 2. 3. 6
⋮

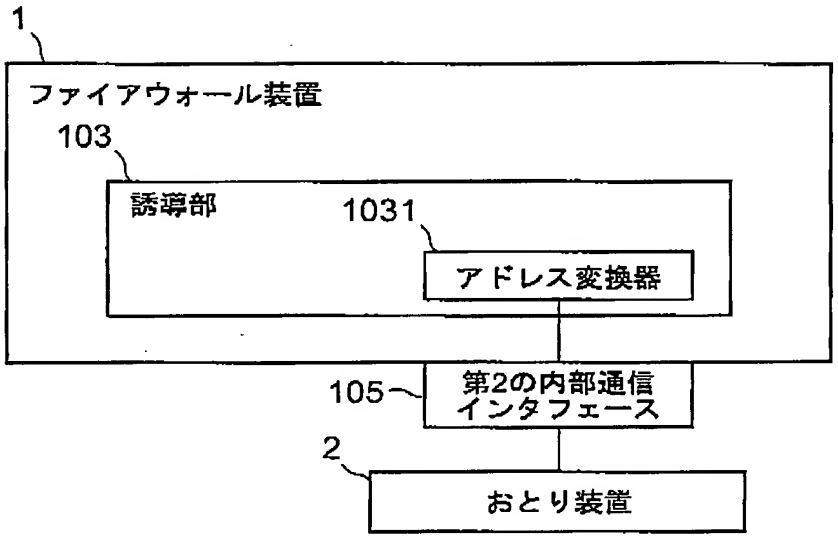
【図 6】


107
防御ルール判定部
攻撃種別
ソースIPアドレス (SRC)
ディスティネーション IPアドレス(DST)
パケットフィルタ処理 (PROC)
RECON
—
—
—
INTRUSION
${SRC_IP_ADDRESS}
*
DROP
DESTRUCTION
${SRC_IP_ADDRESS}
*
DROP
—…無指定(何もしない)
$0…置換用変数

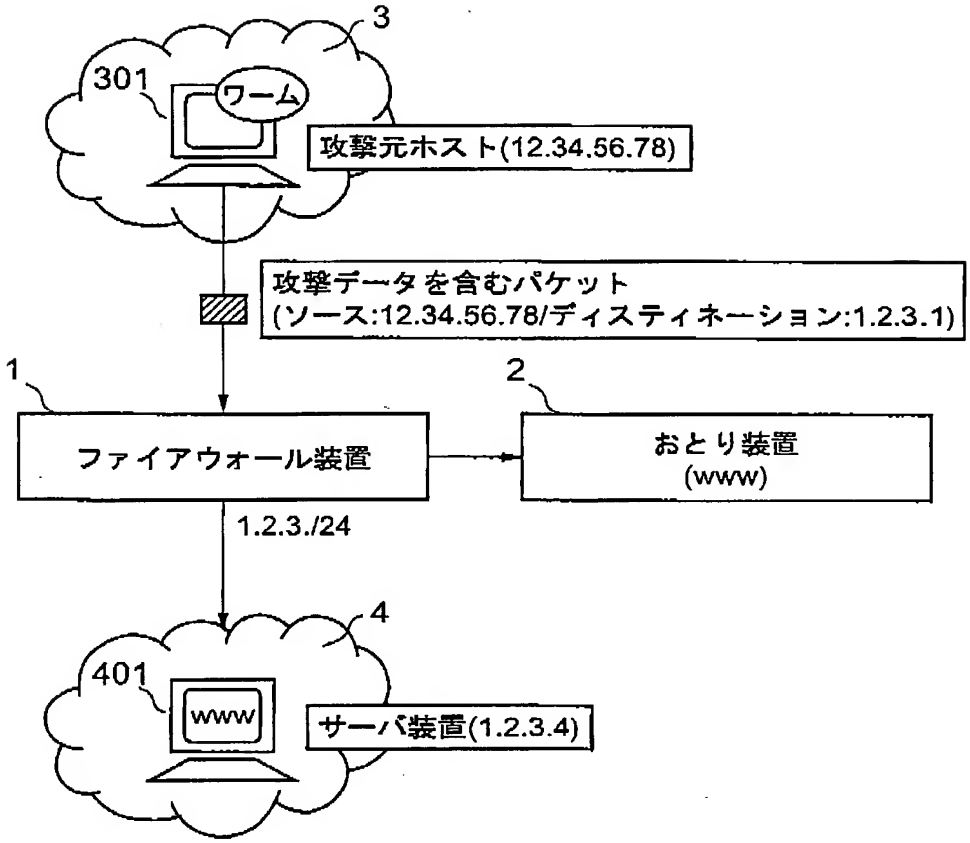
【図 7】


IPパケット受信
A1
IPパケットの受理/廃棄を判定
廃棄
受理
A2
パケットの転送先を決定
おとり
内部ネットワーク
A3
通常のサービスを提供
A4
偽のサービスを提供
A5
攻撃あり？
N
Y
A6
攻撃内容を判定
A7
アクセス制御リストを修正
A8

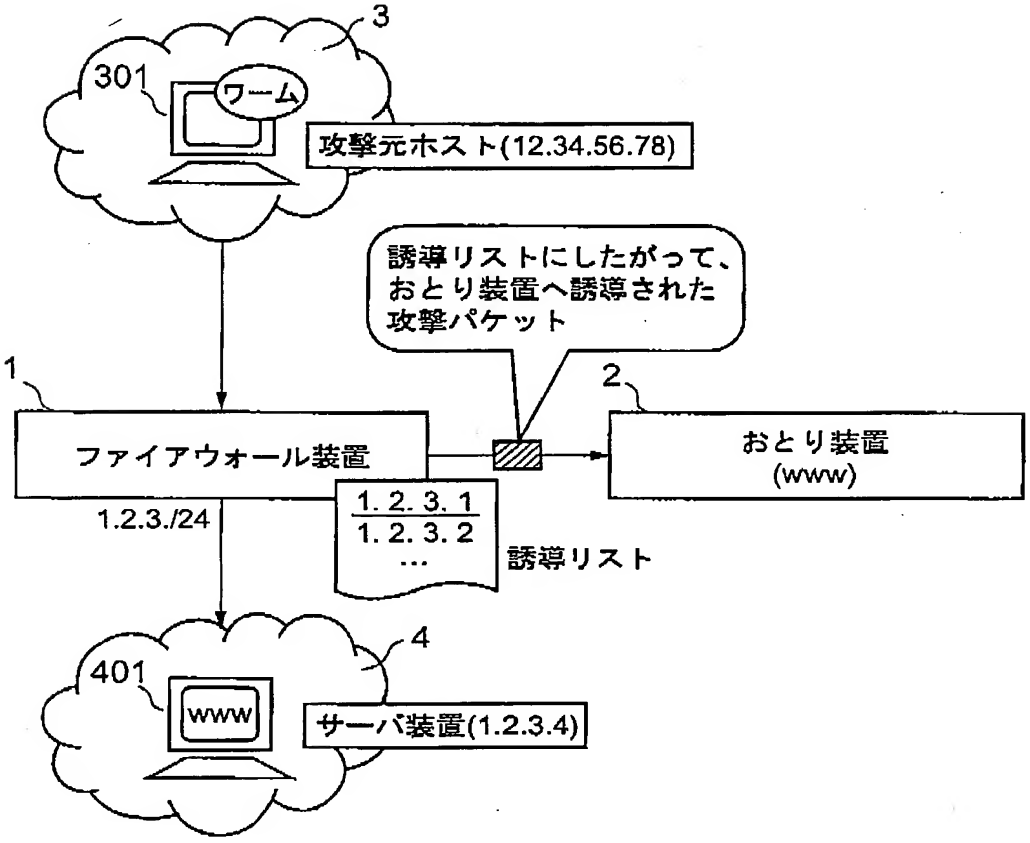
【図 8】


1
ファイアウォール装置
103
誘導部
1031
アドレス変換器
105
第2の内部通信
インタフェース
2
おとり装置

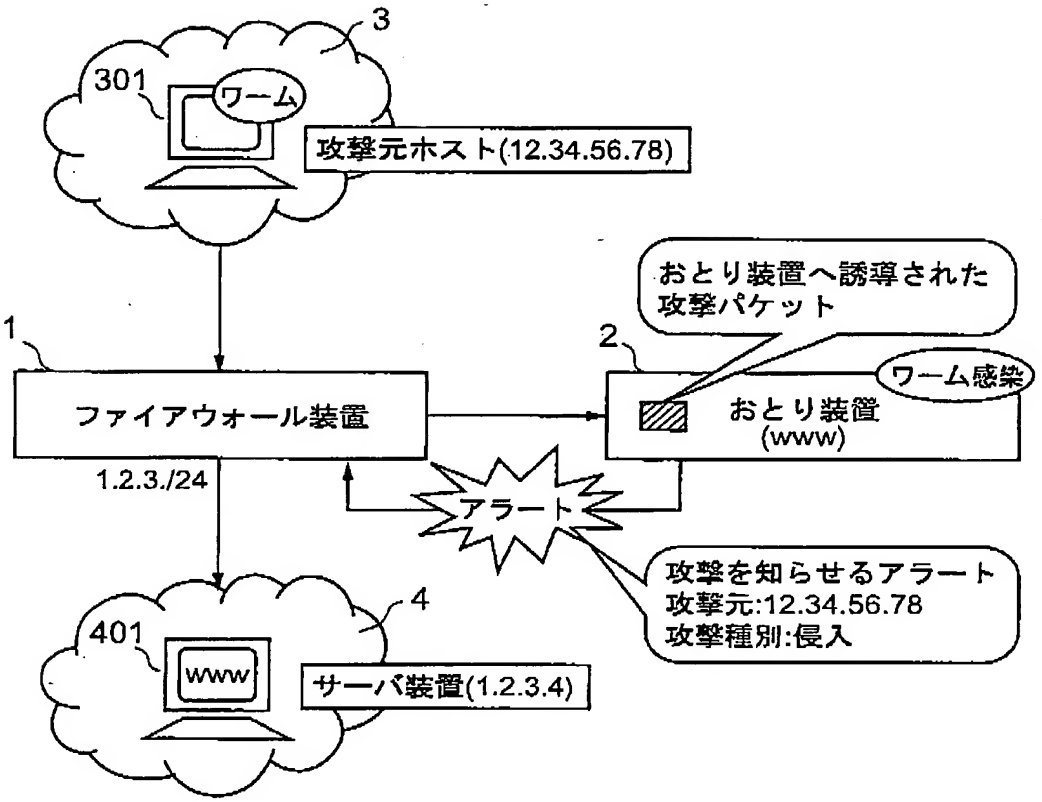
【図 9】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
攻撃データを含むパケット
(ソース:12.34.56.78/ディスティネーション:1.2.3.1)
1
2
ファイアウォール装置
おとり装置
(www)
1.2.3./24
4
401
www
サーバ装置(1.2.3.4)

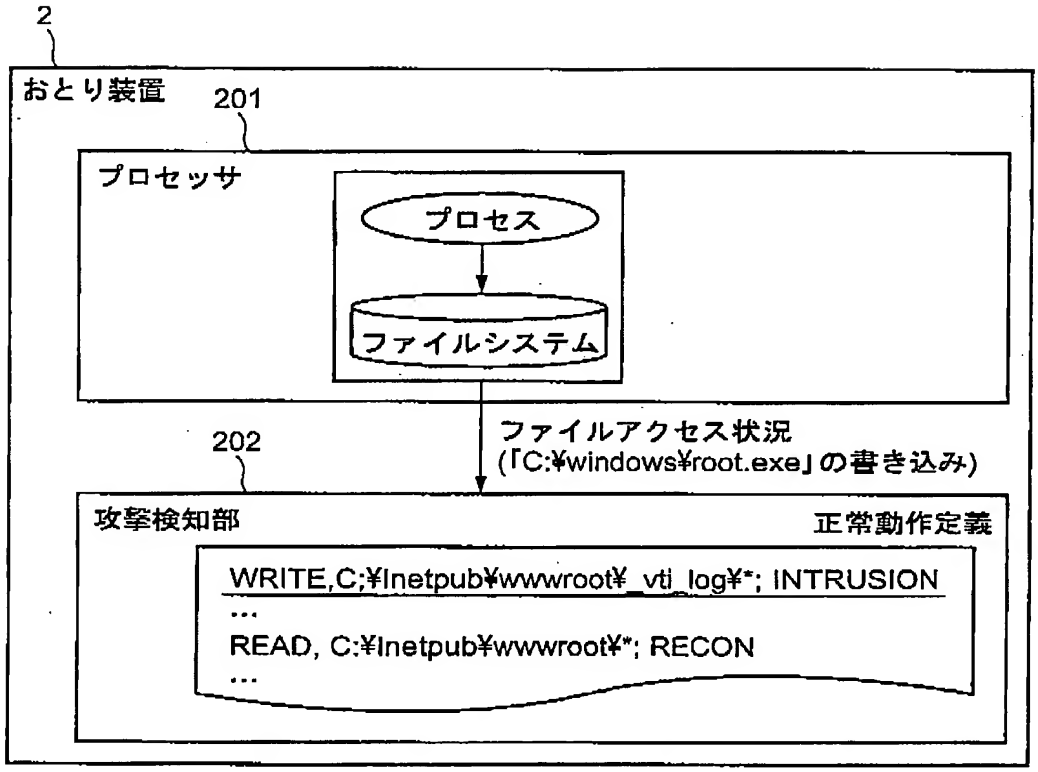
【図10】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
誘導リストにしたがって、
おとり装置へ誘導された
攻撃パケット
1
2
ファイアウォール装置
おとり装置
(www)
1.2.3./24
1. 2. 3. 1
1. 2. 3. 2
…
誘導リスト
4
401
www
サーバ装置(1.2.3.4)

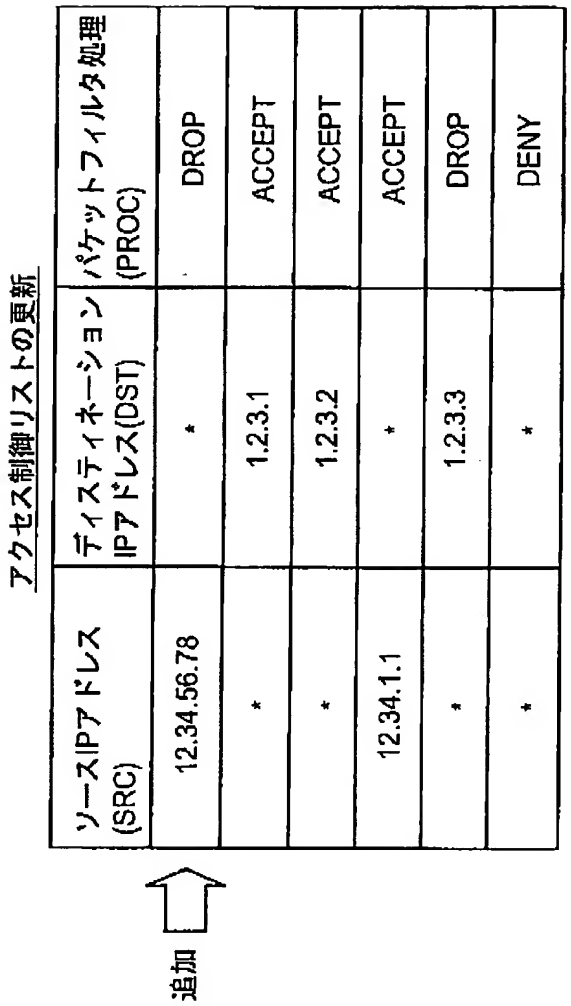
【図11】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
おとり装置へ誘導された
攻撃パケット
1
2
ワーム感染
ファイアウォール装置
おとり装置
(www)
1.2.3./24
アラート
攻撃を知らせるアラート
攻撃元:12.34.56.78
攻撃種別:侵入
4
401
www
サーバ装置(1.2.3.4)

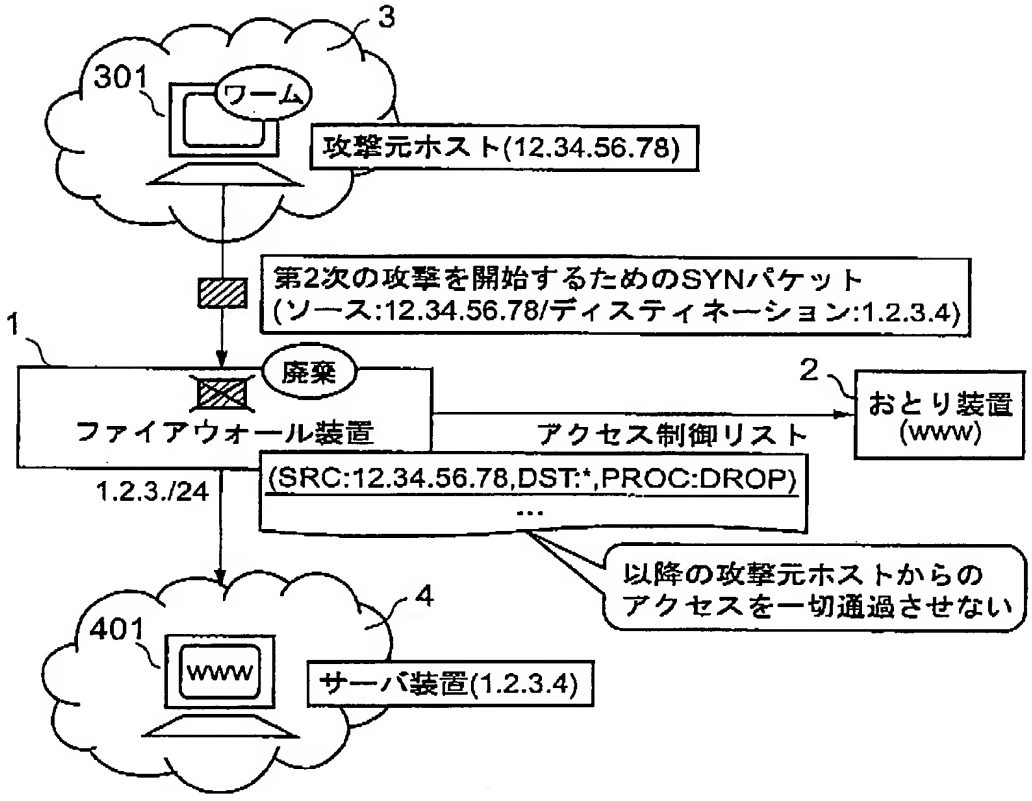
【図12】


2
おとり装置
201
プロセッサ
プロセス
ファイルシステム
ファイルアクセス状況
(「C:¥windows¥root.exe」の書き込み)
202
攻撃検知部
正常動作定義
WRITE,C;¥Inetpub¥wwwroot¥_vti_log¥*; INTRUSION
...
READ, C:¥Inetpub¥wwwroot¥*; RECON
...

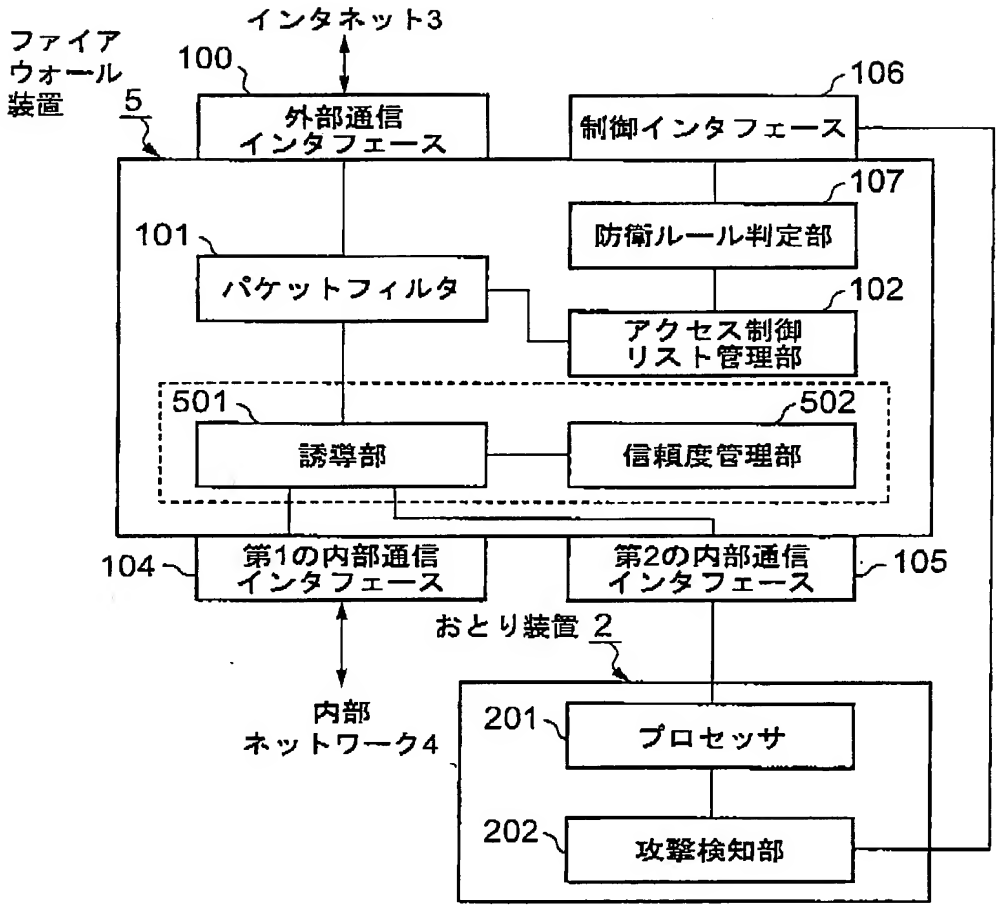
【図13】


アクセス制御リストの更新
ソースIPアドレス (SRC)
ディスティネーション IPアドレス(DST)
パケットフィルタ処理 (PROC)
12.34.56.78
*
DROP
*
1.2.3.1
ACCEPT
*
1.2.3.2
ACCEPT
12.34.1.1
*
ACCEPT
*
1.2.3.3
DROP
*
*
DENY
追加

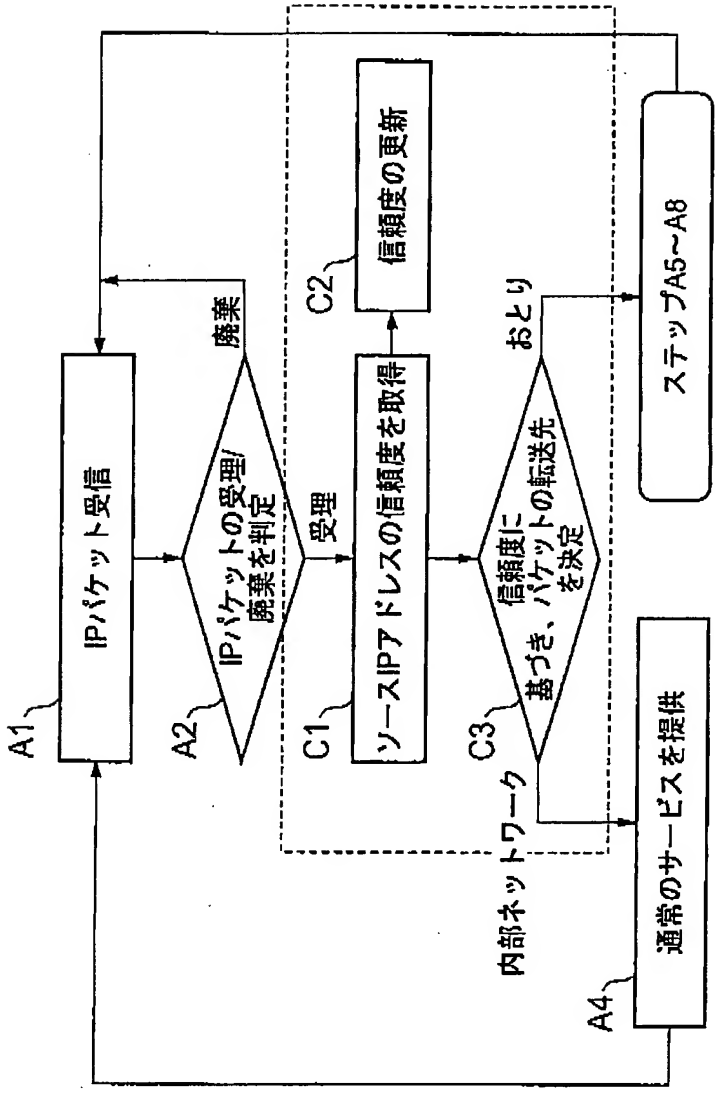
【図14】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
第2次の攻撃を開始するためのSYNパケット
(ソース:12.34.56.78/ディスティネーション:1.2.3.4)
1
廃棄
ファイアウォール装置
2
おとり装置
(www)
アクセス制御リスト
(SRC:12.34.56.78,DST:*,PROC:DROP)
...
1.2.3./24
以降の攻撃元ホストからの
アクセスを一切通過させない
4
401
www
サーバ装置(1.2.3.4)

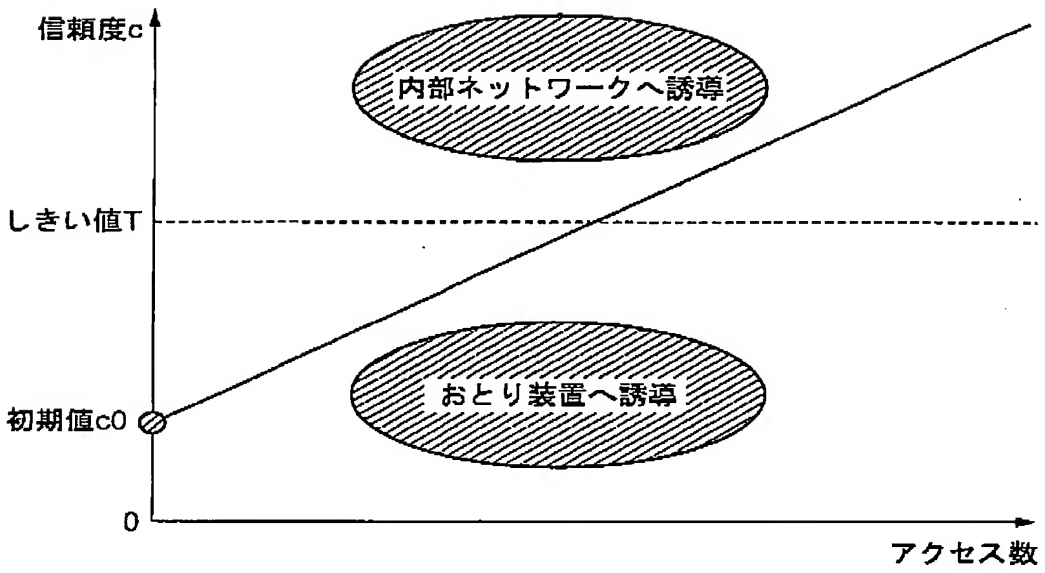
【図15】


インタネット3
ファイア
ウォール
装置
5
100
外部通信
インタフェース
106
制御インタフェース
107
防衛ルール判定部
101
パケットフィルタ
102
アクセス制御
リスト管理部
501
誘導部
502
信頼度管理部
104
第1の内部通信
インタフェース
第2の内部通信
インタフェース
105
おとり装置 2
内部
ネットワーク4
201
プロセッサ
202
攻撃検知部

【図16】

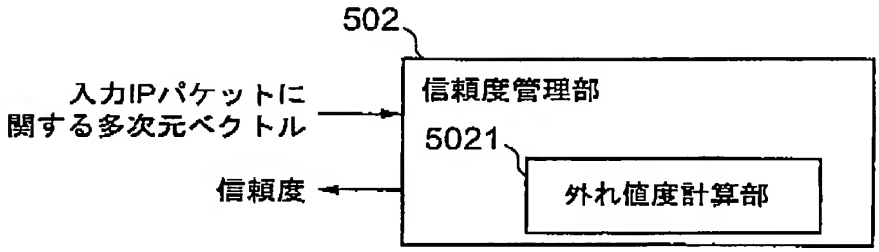

IPパケット受信
A1
IPパケットの受理/廃棄を判定
A2
廃棄
受理
ソースIPアドレスの信頼度を取得
C1
信頼度の更新
C2
信頼度に基づき、パケットの転送先を決定
C3
おとり
ステップA5～A8
内部ネットワーク
通常のサービスを提供
A4

【図17】

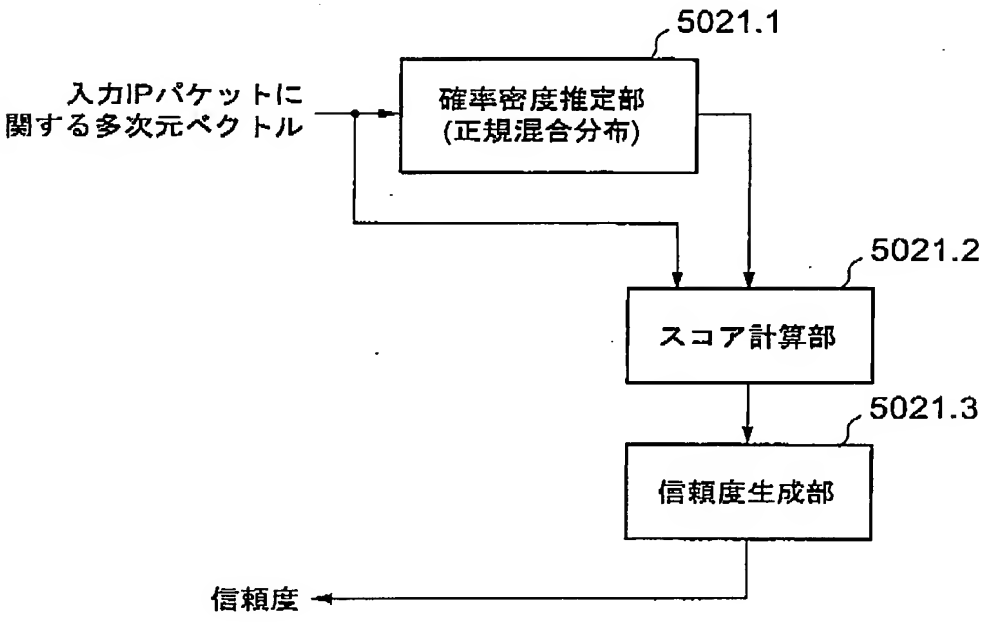


【図18】

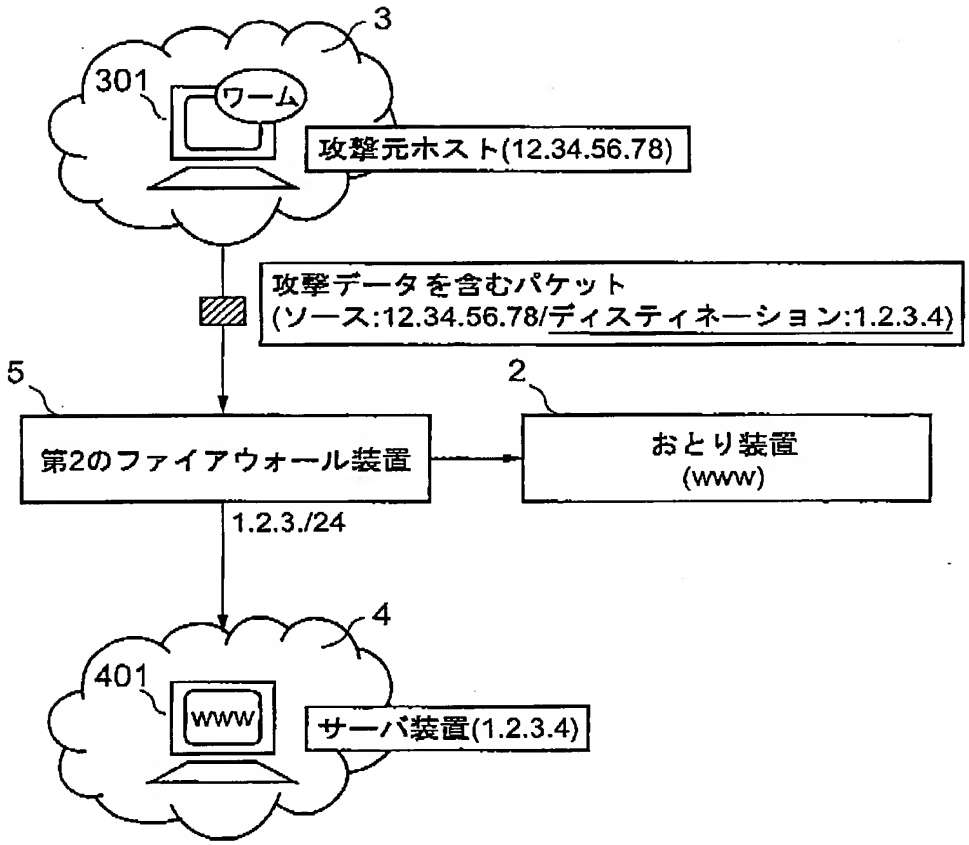
(A)


502
信頼度管理部
入力IPパケットに
関する多次元ベクトル
5021
外れ値度計算部
信頼度

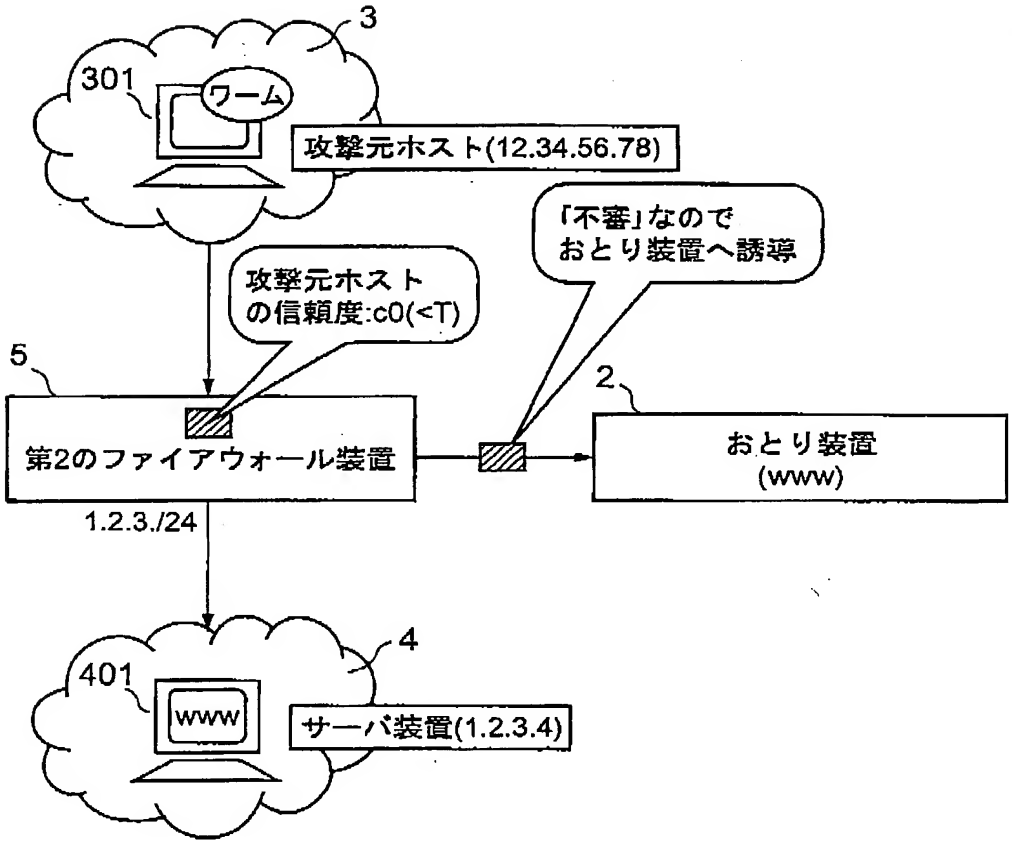
(B)


5021.1
入力IPパケットに
関する多次元ベクトル
確率密度推定部
(正規混合分布)
5021.2
スコア計算部
5021.3
信頼度生成部
信頼度

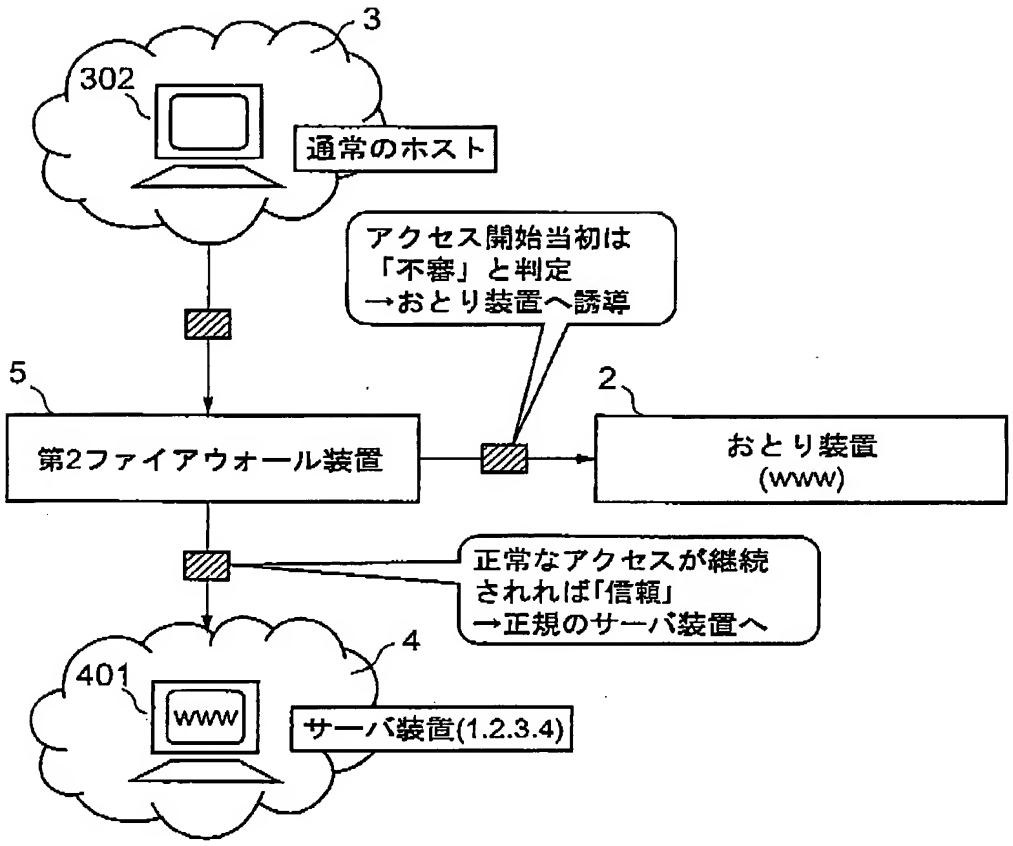
【図19】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
攻撃データを含むパケット
(ソース:12.34.56.78/ディスティネーション:1.2.3.4)
5
2
第2のファイアウォール装置
おとり装置
(www)
1.2.3./24
4
401
www
サーバ装置(1.2.3.4)

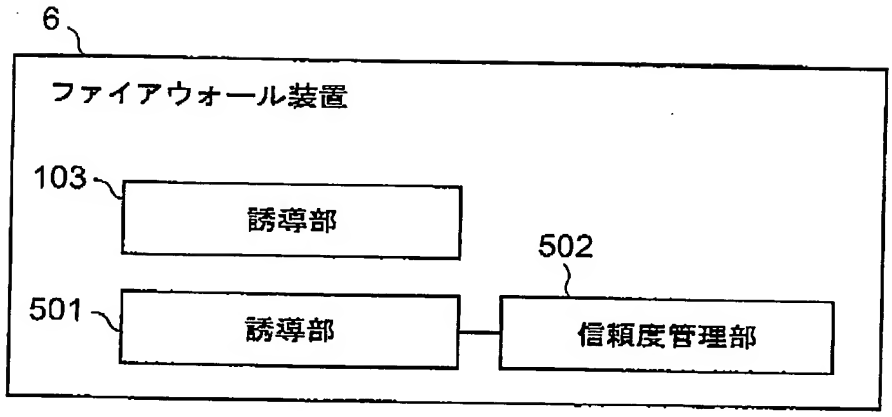
【図20】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
「不審」なので
おとり装置へ誘導
攻撃元ホスト
の信頼度:c0(<T)
5
2
第2のファイアウォール装置
おとり装置
(www)
1.2.3./24
4
401
www
サーバ装置(1.2.3.4)

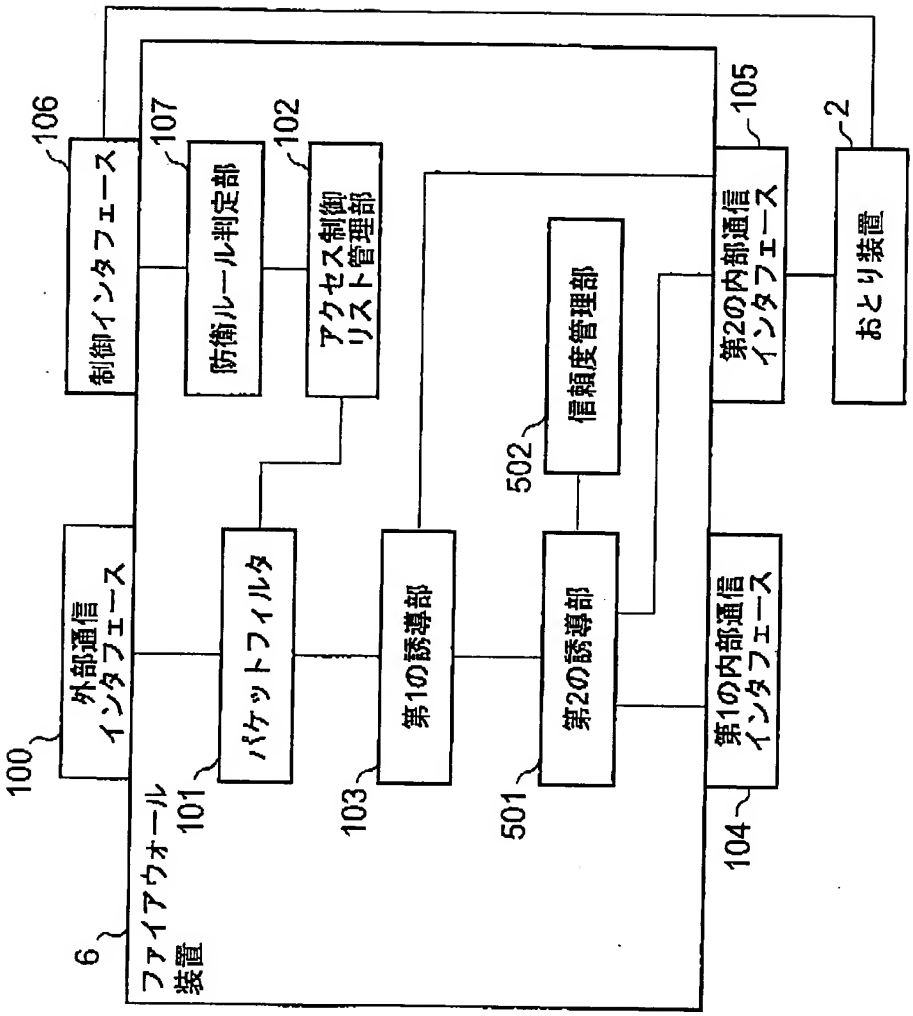
【図21】


3
302
通常のホスト
アクセス開始当初は
「不審」と判定
→おとり装置へ誘導
5
2
第2ファイアウォール装置
おとり装置
(www)
正常なアクセスが継続
されれば「信頼」
→正規のサーバ装置へ
4
401
www
サーバ装置(1.2.3.4)

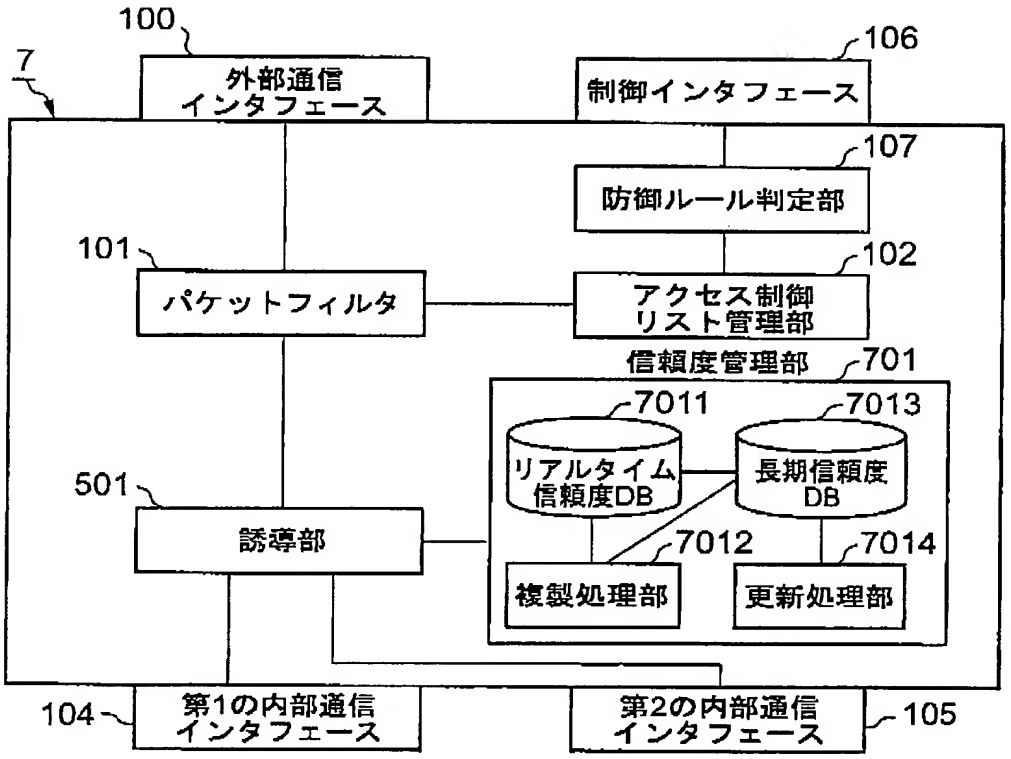
【図22】



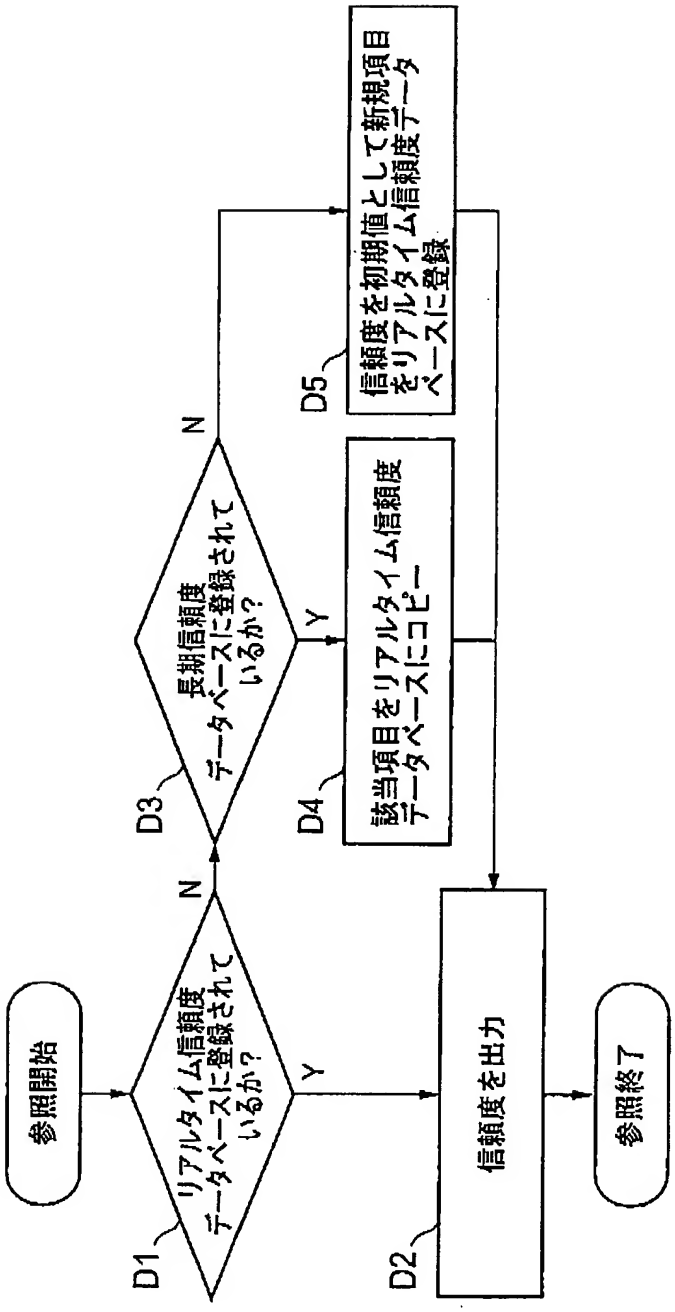
【図23】


106
107
102
105
2
制御インタフェース
防御ルール判定部
アクセス制御
リスト管理部
第2の内部通信
インタフェース
おとり装置
502
信頼度管理部
外部通信
インタフェース
パケットフィルタ
第1の誘導部
第2の誘導部
第1の内部通信
インタフェース
100
101
103
501
104
6
ファイアウォール
装置

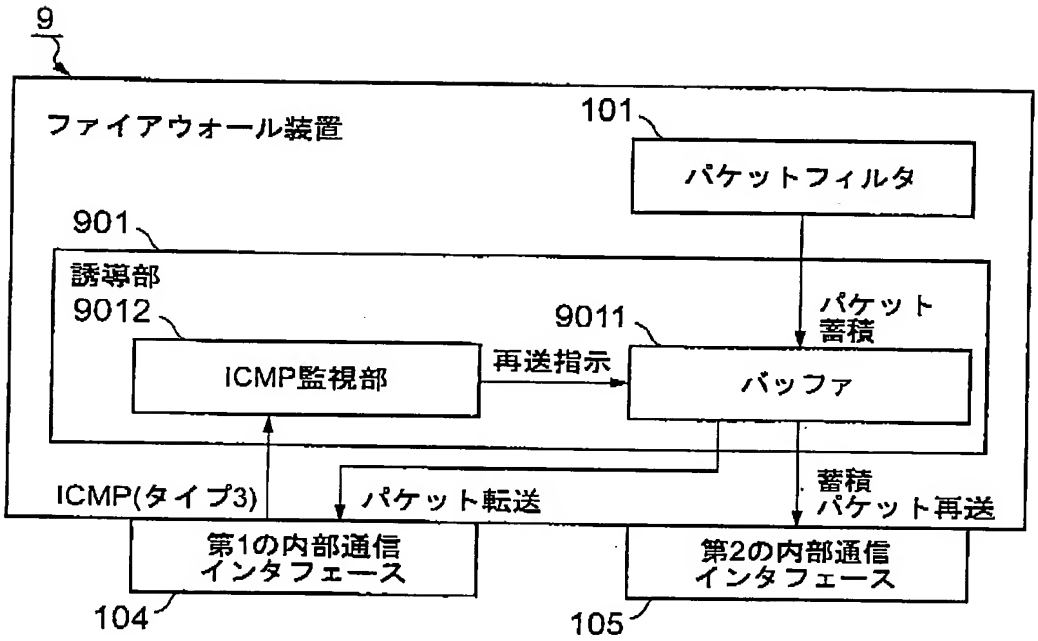
【図24】


100
外部通信
インタフェース
7
106
制御インタフェース
107
防御ルール判定部
101
パケットフィルタ
102
アクセス制御
リスト管理部
信頼度管理部
701
7011
7013
リアルタイム
信頼度DB
長期信頼度
DB
501
誘導部
7012
7014
複製処理部
更新処理部
104
第1の内部通信
インタフェース
第2の内部通信
インタフェース
105

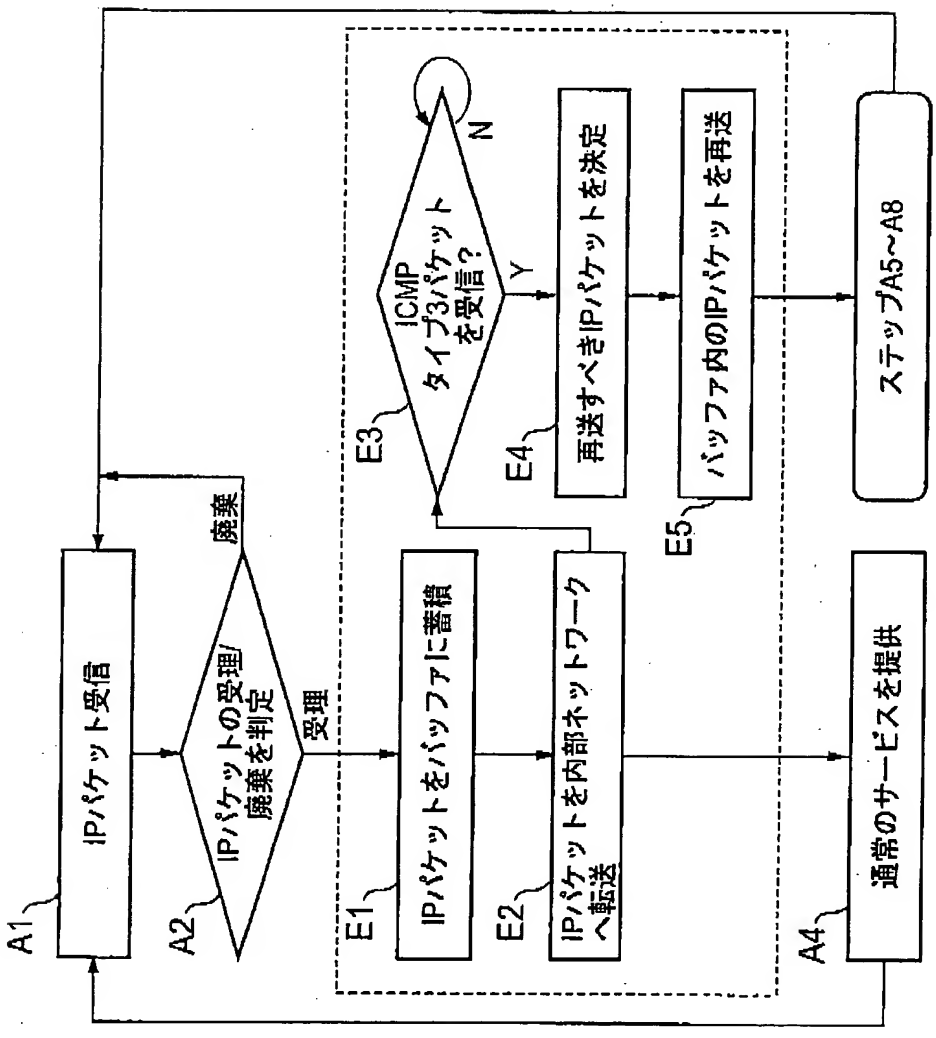
【図25】


参照開始
D1
リアルタイム信頼度データベースに登録されているか？
N
Y
D3
長期信頼度データベースに登録されているか？
N
Y
D4
該当項目をリアルタイム信頼度データベースにコピー
D5
信頼度を初期値として新規項目をリアルタイム信頼度データベースに登録
D2
信頼度を出力
参照終了

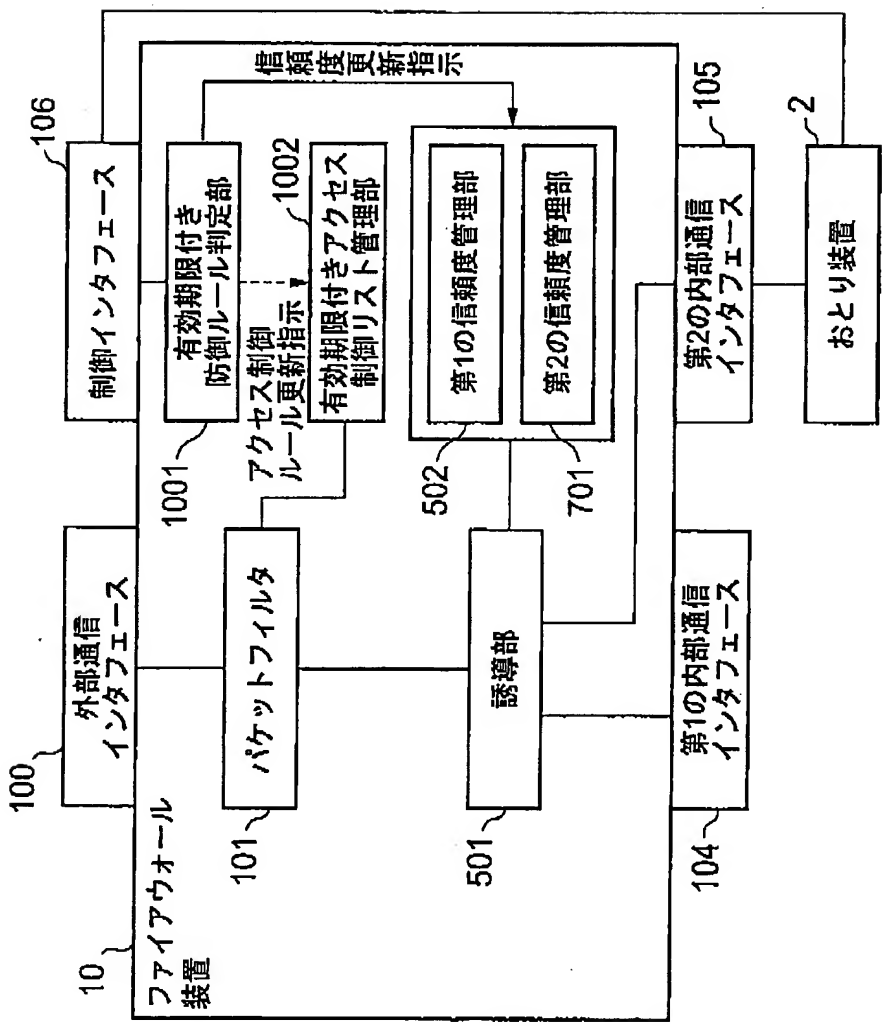
【図26】


9
ファイアウォール装置
101
パケットフィルタ
901
誘導部
9012
ICMP監視部
9011
バッファ
再送指示
パケット
蓄積
ICMP(タイプ3)
パケット転送
蓄積
パケット再送
第1の内部通信
インタフェース
第2の内部通信
インタフェース
104
105

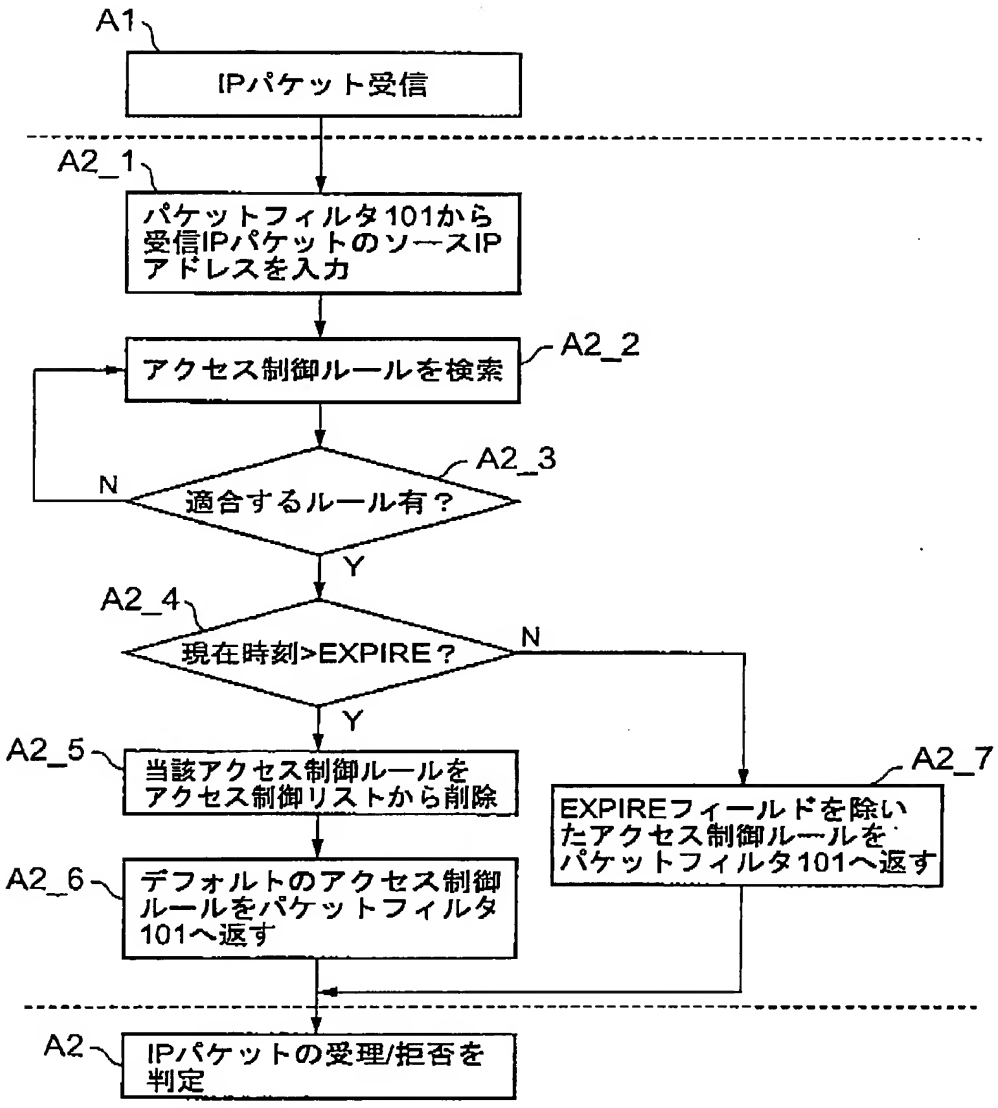
【図27】


IPパケット受信
A1
IPパケットの受理/廃棄を判定
A2
廃棄
受理
IPパケットをバッファに蓄積
E1
IPパケットを内部ネットワークへ転送
E2
ICMPタイプ3パケットを受信?
E3
N
Y
再送すべきIPパケットを決定
E4
バッファ内のIPパケットを再送
E5
ステップA5~A8
通常のサービスを提供
A4

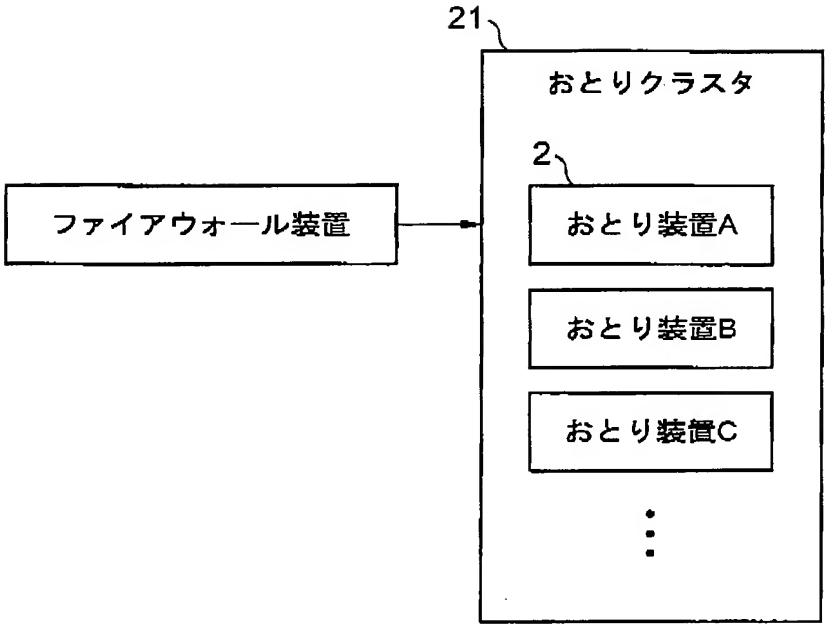
【図28】


信頼度更新指示
106
制御インタフェース
有効期限付き防御ルール判定部
1002
有効期限付きアクセス制御リスト管理部
第1の信頼度管理部
第2の信頼度管理部
105
第2の内部通信インタフェース
2
おとり装置
1001
アクセス制御ルール更新指示
502
701
外部通信インタフェース
パケットフィルタ
誘導部
第1の内部通信インタフェース
100
101
501
104
ファイアウォール装置
10

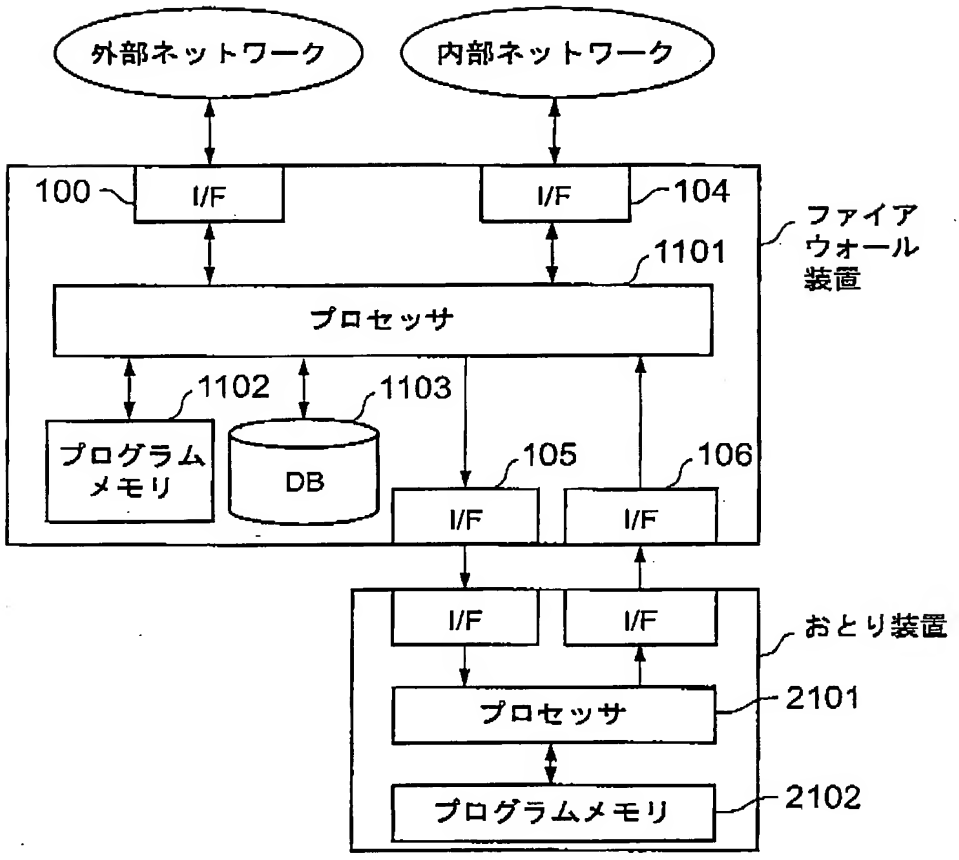
【図29】


A1
IPパケット受信
A2_1
パケットフィルタ101から受信IPパケットのソースIPアドレスを入力
アクセス制御ルールを検索
A2_2
A2_3
適合するルール有？
N
Y
A2_4
現在時刻>EXPIRE？
N
Y
A2_5
当該アクセス制御ルールをアクセス制御リストから削除
A2_6
デフォルトのアクセス制御ルールをパケットフィルタ101へ返す
A2_7
EXPIREフィールドを除いたアクセス制御ルールをパケットフィルタ101へ返す
A2
IPパケットの受理/拒否を判定

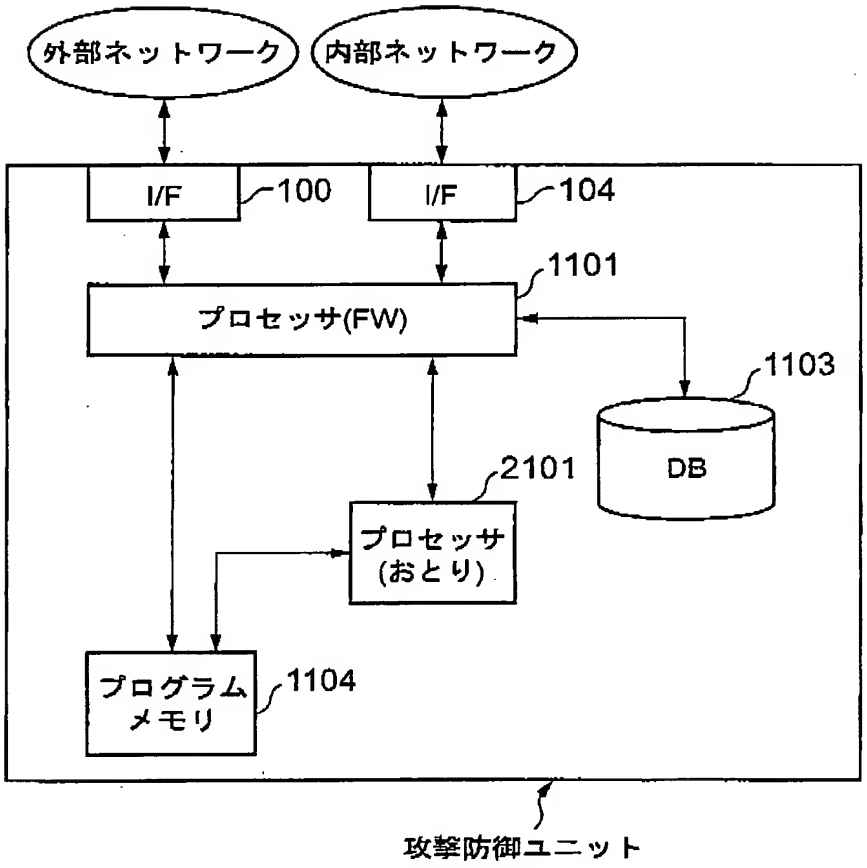
【図30】



【図31】

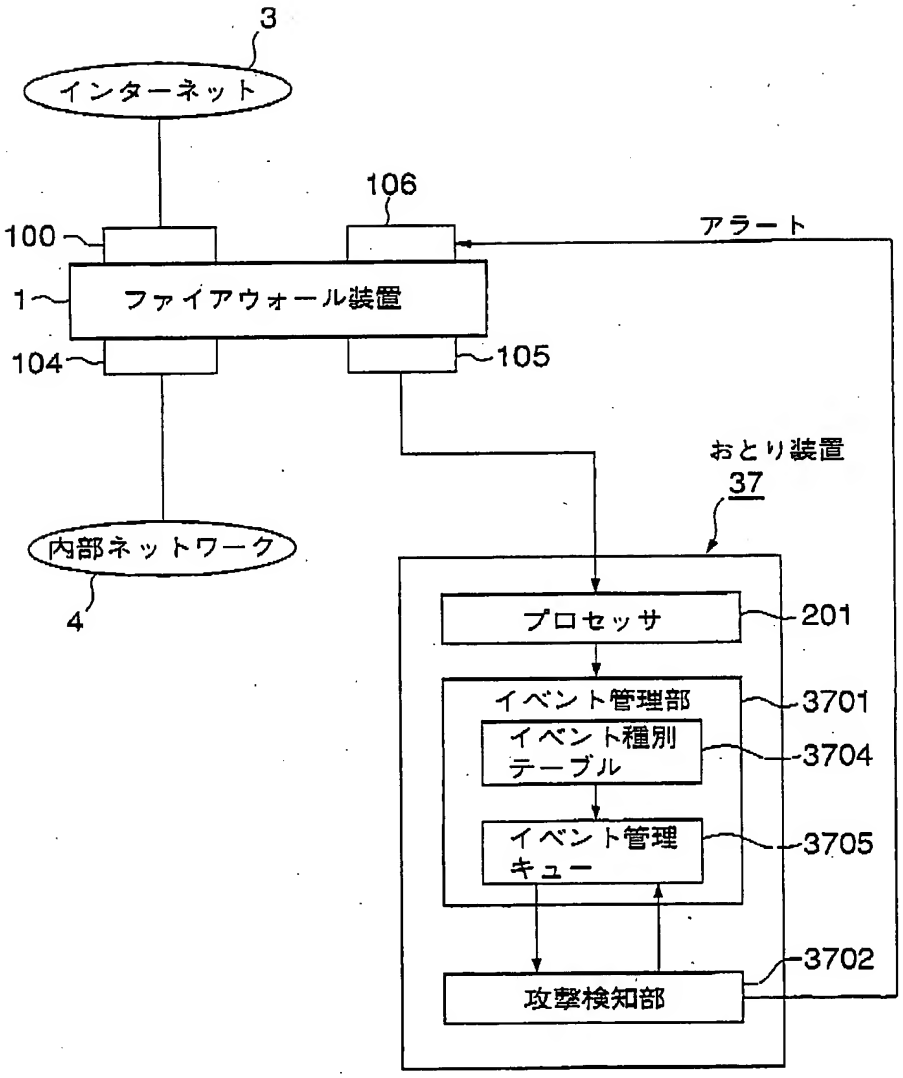

外部ネットワーク
内部ネットワーク
100
I/F
I/F
104
ファイア
ウォール
装置
1101
プロセッサ
1102
1103
プログラム
メモリ
DB
105
106
I/F
I/F
I/F
I/F
おとり装置
2101
プロセッサ
2102
プログラムメモリ

【図32】


外部ネットワーク
内部ネットワーク
I/F
100
I/F
104
1101
プロセッサ(FW)
1103
DB
2101
プロセッサ
(おとり)
プログラム
メモリ
1104
攻撃防御ユニット

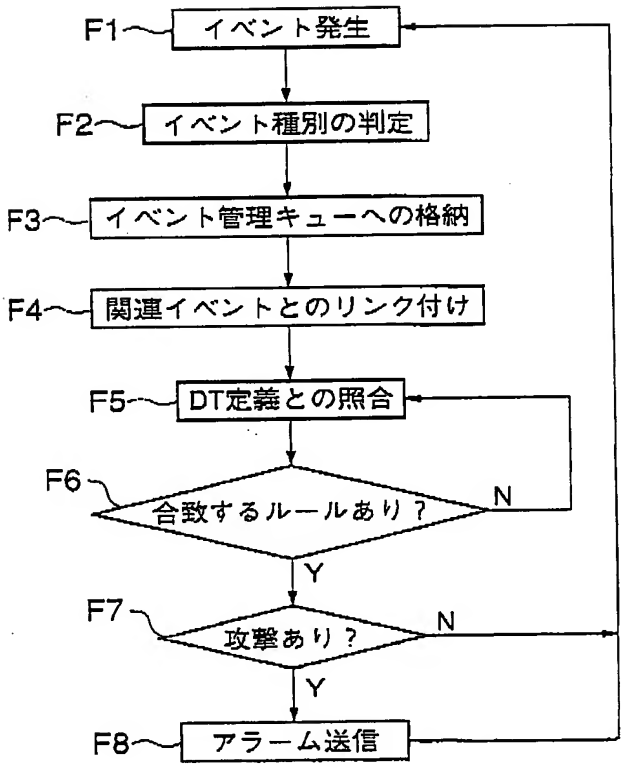
00537

図33


3
インターネット
106
100
アラート
ファイアウォール装置
1
104
105
おとり装置
37
内部ネットワーク
4
プロセッサ
201
イベント管理部
3701
イベント種別テーブル
3704
イベント管理キュー
3705
3702
攻撃検知部

00537

図34


F1
イベント発生
F2
イベント種別の判定
F3
イベント管理キューへの格納
F4
関連イベントとのリンク付け
F5
DT定義との照合
F6
合致するルールあり？
N
Y
F7
攻撃あり？
N
Y
F8
アラーム送信

00537

図35

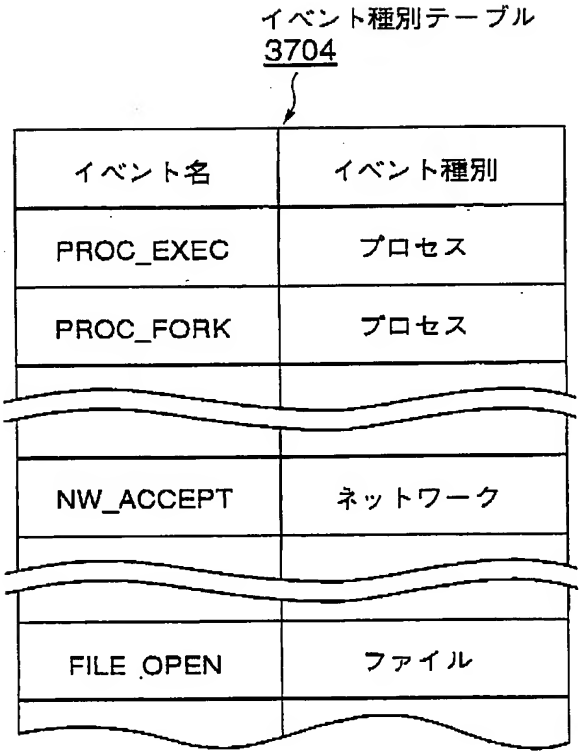


図36

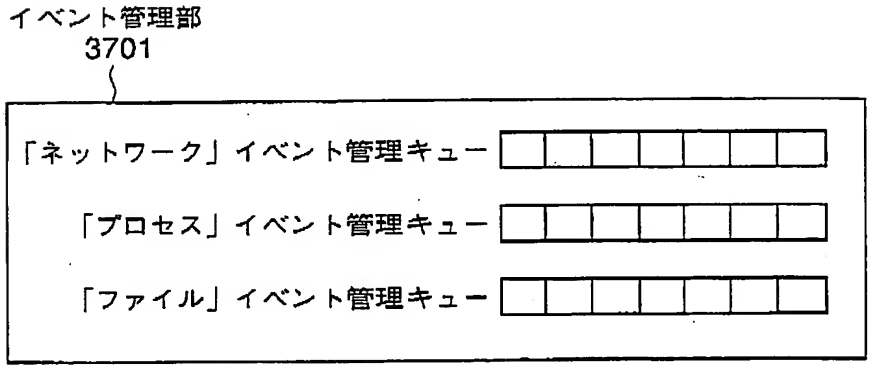


図37

H1
カレントイベントに記載された発行源プロセスのプロセスID (PID) を抽出する
H2
プロセスイベント管理キューの最後尾のイベントを参照する
H3
プロセス生成イベントか？
Y
N
H4
1つ前方のイベントを参照する
H5
プロセスIDがPIDに一致するか？
Y
N
H6
現在参照しているイベントから、カレントイベントへ順方向リンクを張る
H7
カレントイベントから、現在参照しているイベントへ、逆方向リンクを張る

00537

図38

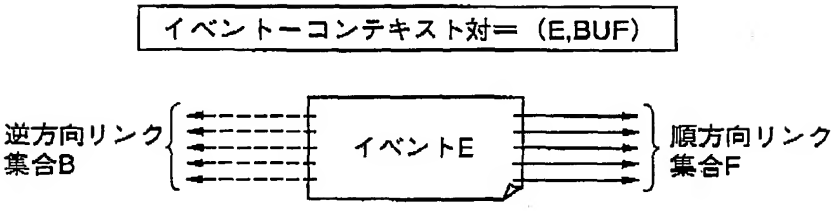


図39

4101 DT定義ファイル

```
#（ルール1）WWWサーバによるログの書き出しを許可する
0.0.0.0/0,<inetinfo.exe>,FILE_WRITE,C:¥winnt¥system32¥LogFiles¥.*;ALLOW
#（ルール2）WWWサーバによるコンテンツ領域の読込みを許可する。
0.0.0.0/0,<inetinfo.exe>,FILE_READ,C;¥Inetpub¥wwwroot¥,*;ALLOW

#（ルール3）WWWサーバのサブシステムである登録CGIはデータベースを更新してよい。
0.0.0.0/0,<inetinfo.exe><regist.exe>$,FILE_WRITE,C:¥data¥client.db;ALLOW
#（ルール4）WWWサーバのサブシステムである出力CGIによるデータベース読込みを許可。
0.0.0.0/0,<inetinfo.exe><view.exe>$,FILE_READ,C:¥data¥client.db;ALLOW

#（ルール5）FTPサーバはコンテンツ領域に書き出し可能
#ただし、管理者ドメイン10.56.192.0/24からのアクセスに限る
10.56.192.0/24.^<ftpd.exe>+$,FILE_WRITE,C:¥Inetpub¥wwwroot¥.*;ALLOW

#（ルール6）WWWサーバは、特に許可されていない限り、ファイル書き出しを行わない。
0.0.0.0/0,<inetinfo.exe>.FILE_WRITE,.*;DENY
#（ルール7）許可されたプログラム以外によるデータベース領域のアクセスを禁止する。
0.0.0.0/0,*.*,FILE_READ|FILE_WRITE,C:¥data¥.*;DENY
#（ルール8）許可されたプログラム以外によるコンテンツ領域の書換えは攻撃である。
0.0.0.0/0,.*,.*,FILE_WRITE,C:¥Inetpub¥wwwroot¥.*;DENY

#（デフォルトルール）どのルールにもマッチしない場合は「許可」
DEFAULT;ALLOW
```

00537

図40

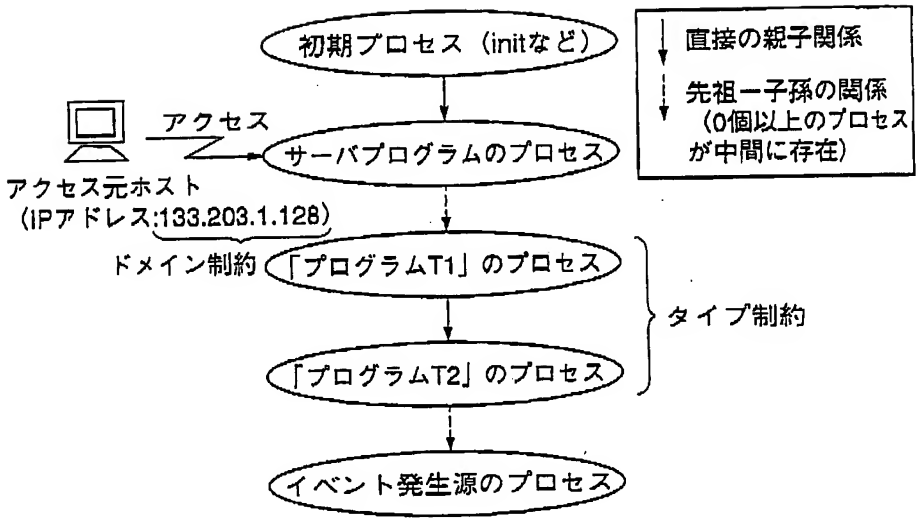
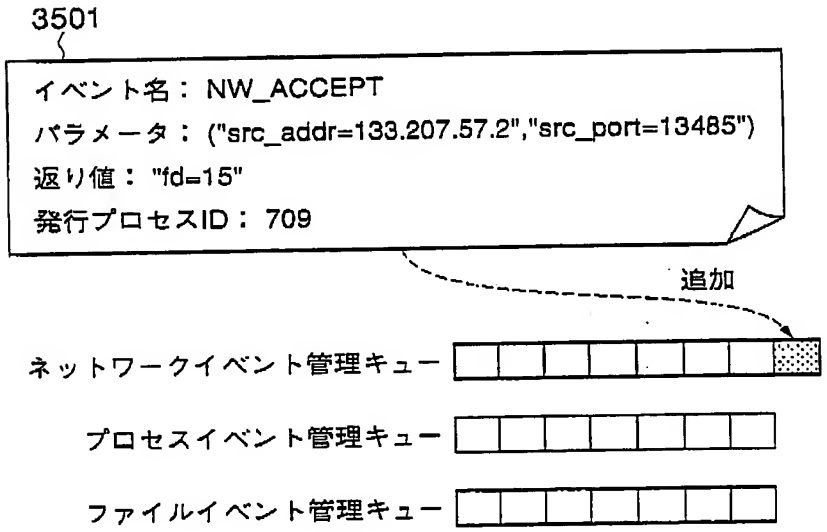


図41



00537

図42

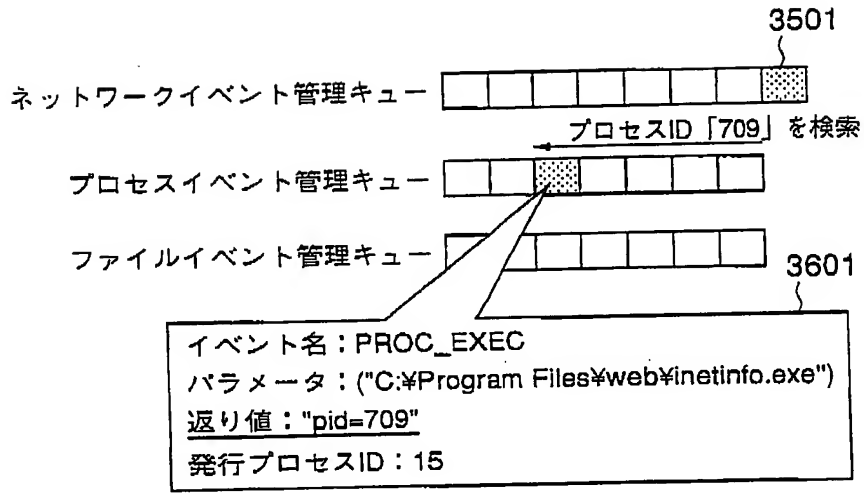
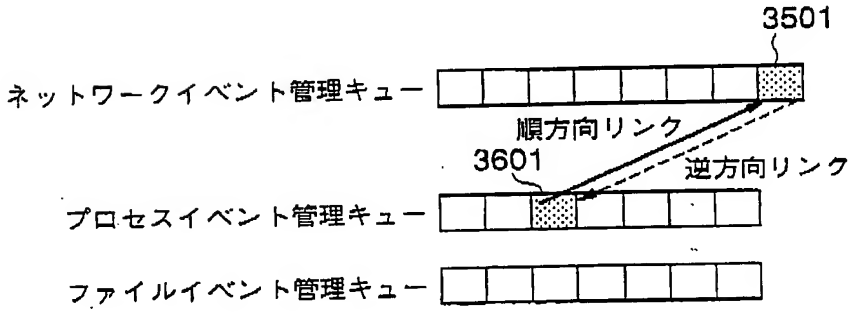


図43



00537

図44

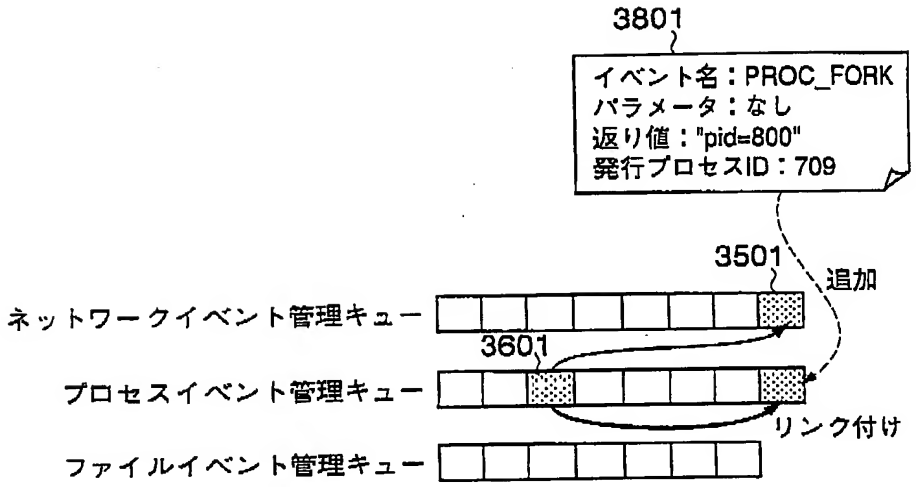
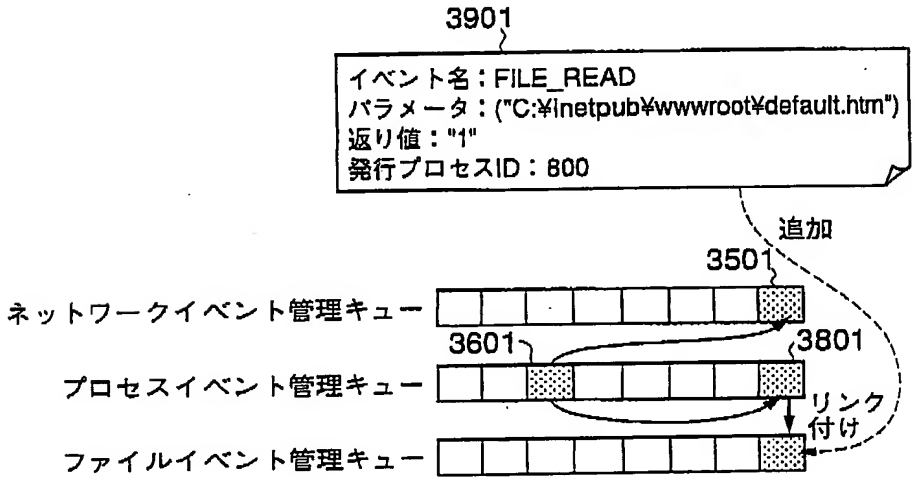


図45



00537

図46

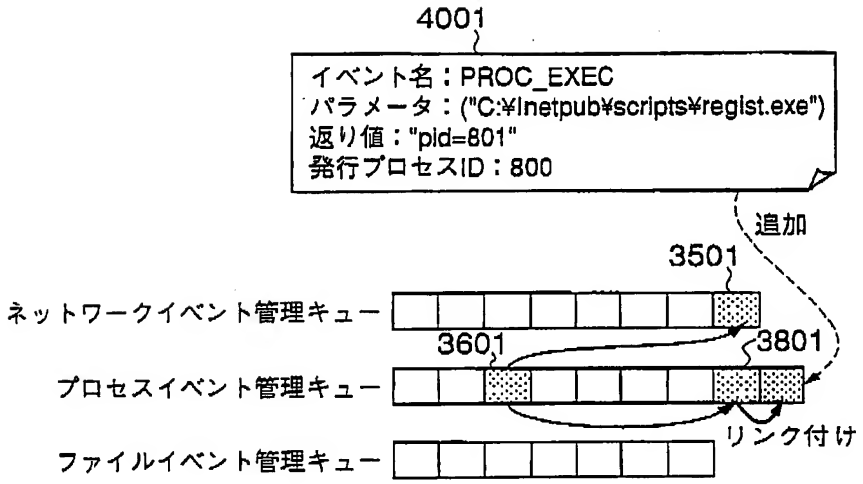
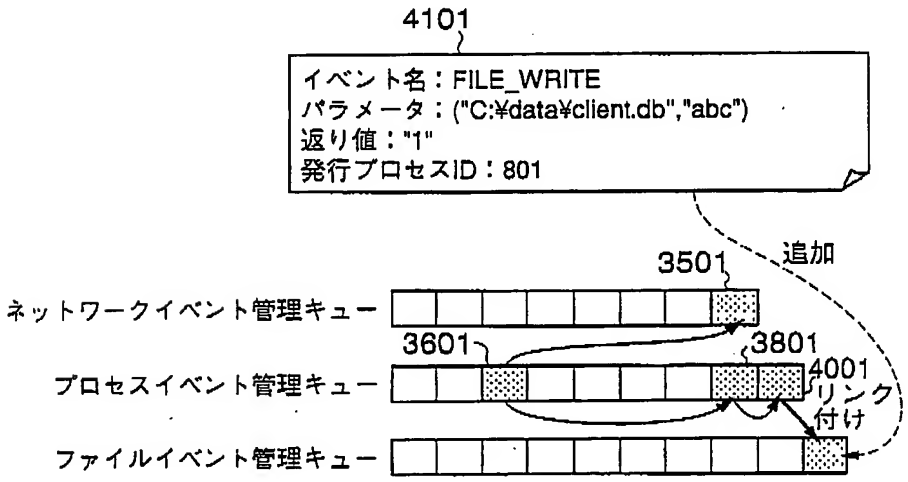


図47



00537

図48

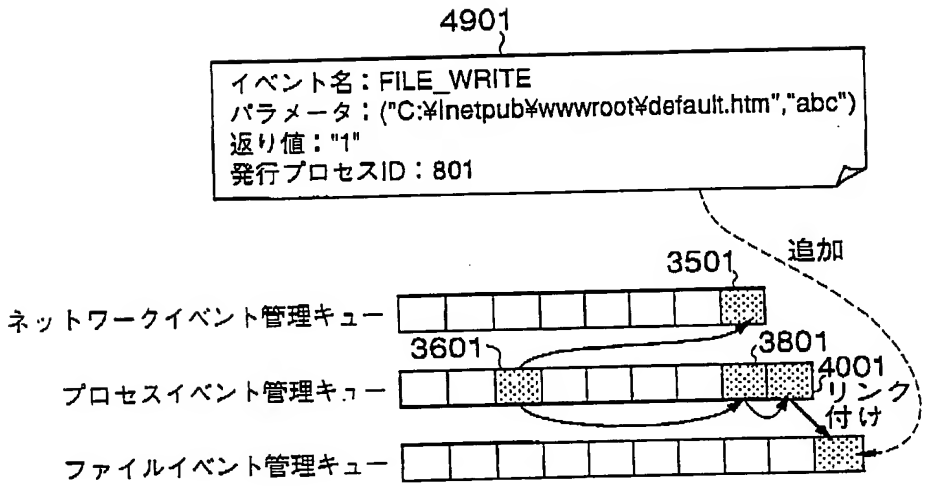
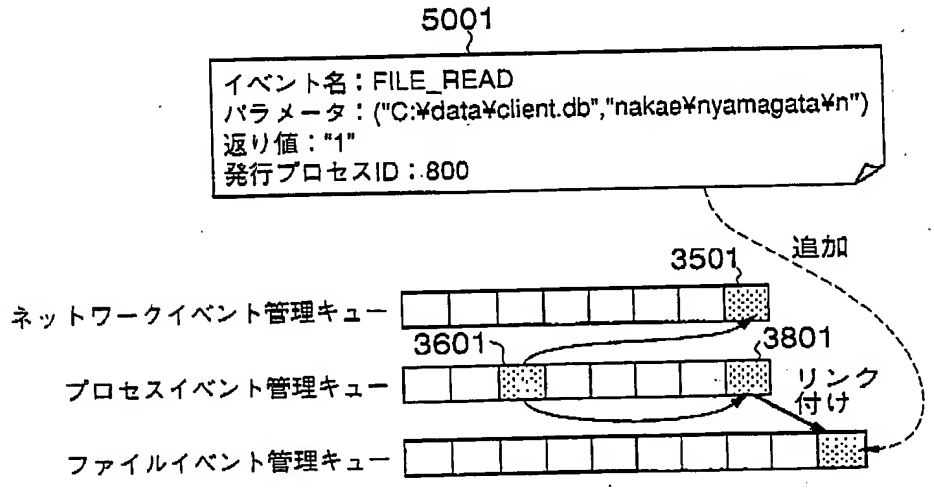


図49



00537

図50

インターネット3
ファイアウォール装置 51
外部通信インターフェース
100
パケットフィルタ
101
アクセス制御リスト管理部
102
仮想サーバ部
5101
信頼度管理部
5102
防御ルール判定部
107
制御インターフェース
106
第1の内部通信インターフェース
104
第2の内部通信インターフェース
105
内部ネットワーク4
おとり装置2

図51

仮想サーバ部
5101
パケットフィルタ
101
接続管理部
5201
信頼度管理部
5102
第1入力バッファ
5202
第1出力バッファ
5203
第2入力バッファ
5204
第2出力バッファ
5205
内部ネットワーク4
おとり装置2

図52

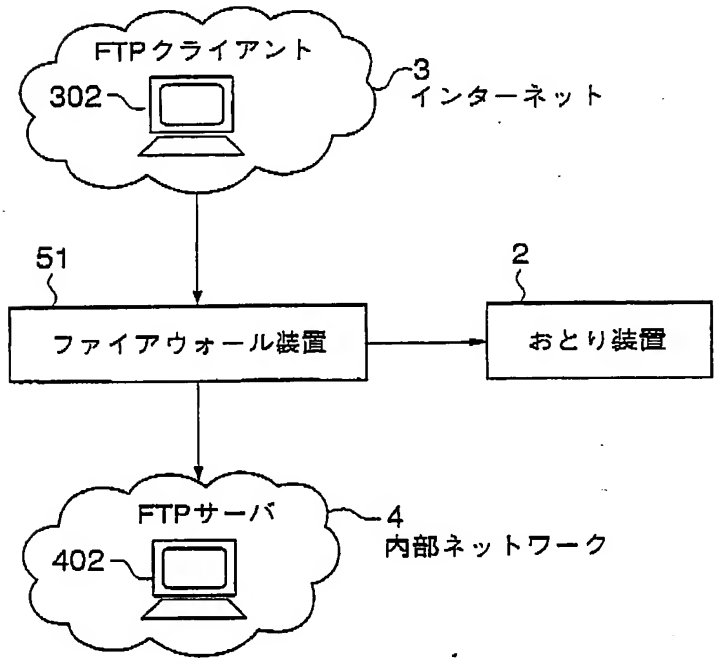
G1
アクセス元ホストとの仮接続を行う
G2
要求データを受信
G3
第1および第2入力バッファに要求データを格納
G4
要求データの信頼度cを取得
G5
c≧T?
Y
N
G6-1
第1および第2入力バッファに要求データ転送を指示
G6-2
第2入力バッファのみに要求データ転送を指示
G7-1
第1出力バッファに応答データあり?
N
Y
G7-2
攻撃あり?
Y
N
G8-1
第1出力バッファ内の応答データをアクセス元ホストに転送
G8-2
第1入力バッファに要求データ転送を指示
G8-3
強制遮断

00537

図53

要求データ	信頼度
D0	1
D1	0
・・・	・・・
Dn	1

図54

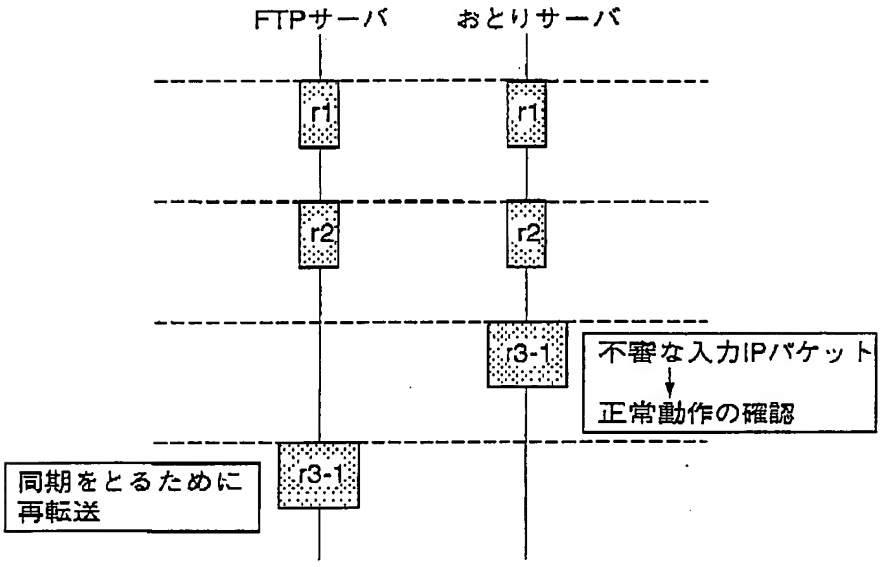


00537

図55

要求データ	信頼度
D0	1
D1	0
. . .	. . .
1	0

図56



00537

図57

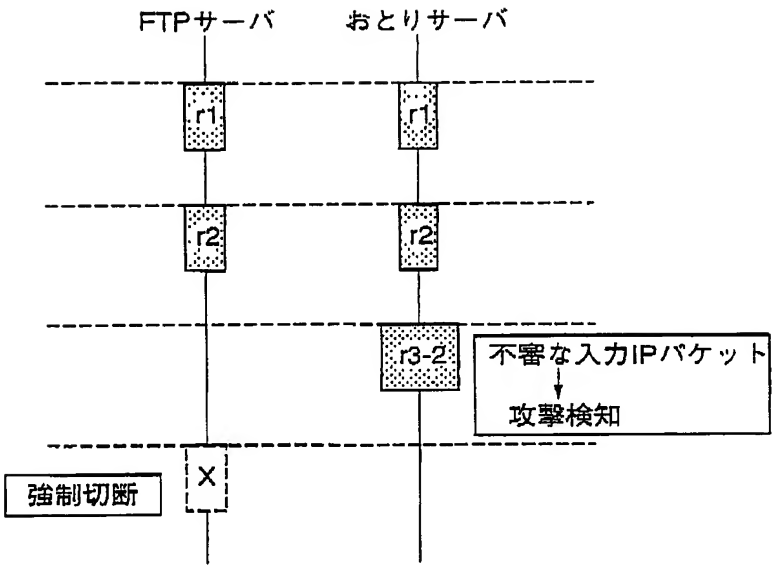


図58

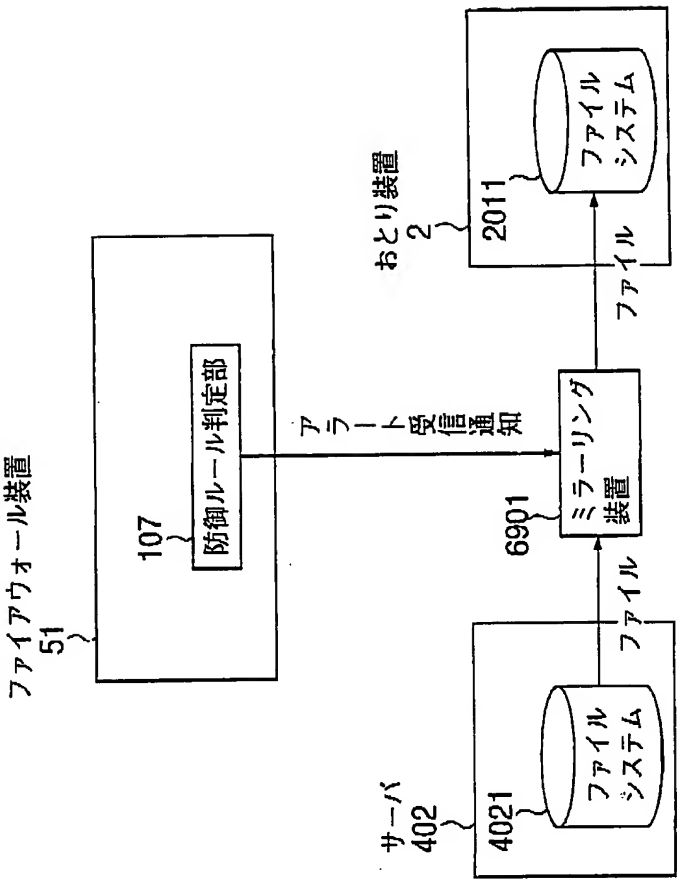

ファイアウォール装置
51
107
防御ルール判定部
アラート受信通知
おとり装置
2
2011
ファイルシステム
ファイル
6901
ミラーリング装置
ファイル
サーバ
402
4021
ファイルシステム

図59

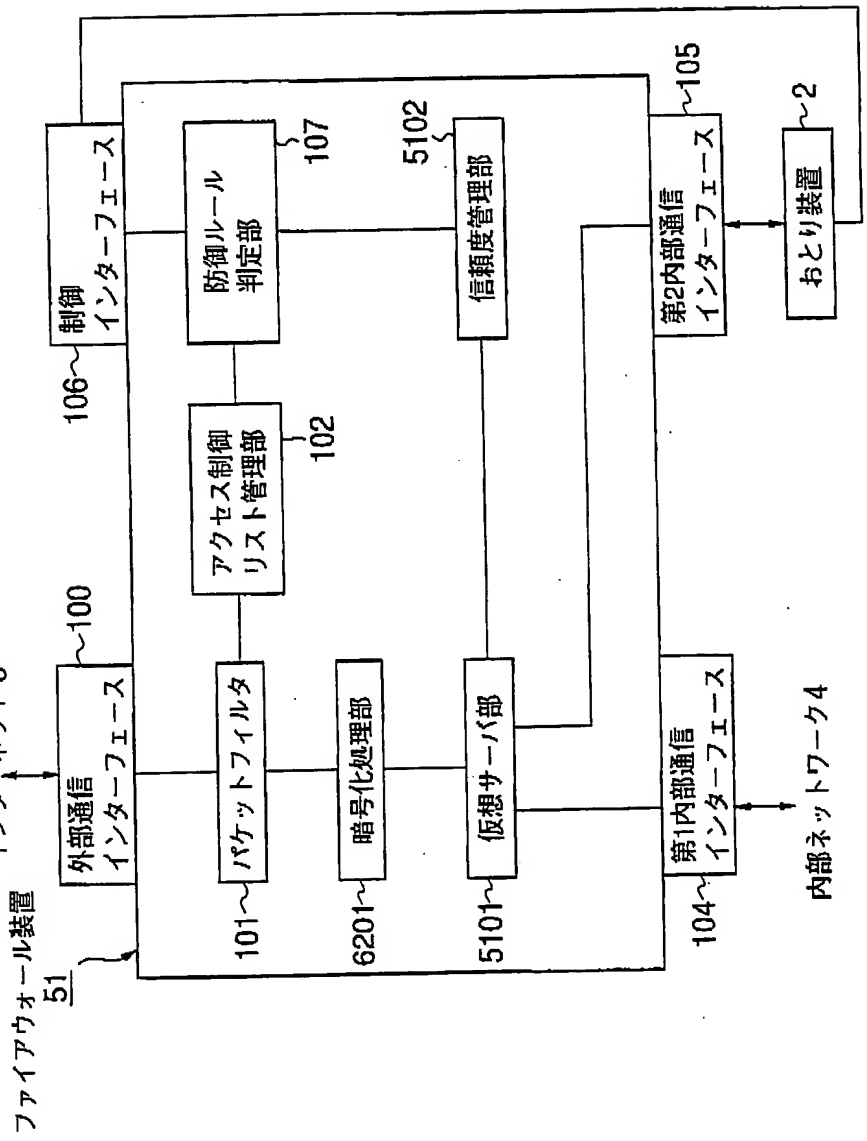

ファイアウォール装置
51
インターネット3
外部通信インターフェース
100
パケットフィルタ
101
アクセス制御リスト管理部
102
暗号化処理部
6201
制御インターフェース
106
防御ルール判定部
107
仮想サーバ部
5101
信頼度管理部
5102
第1内部通信インターフェース
104
第2内部通信インターフェース
105
おとり装置
2
内部ネットワーク4

図60

ファイアウォール装置
7001
インターネット3
101
パケットフィルタ
102
アクセス制御リスト管理部
スイッチ装置
7002
501
誘導部
502
信頼度管理部
107
防御ルール判定部
2
おとり装置
内部ネットワーク4

00537

図61

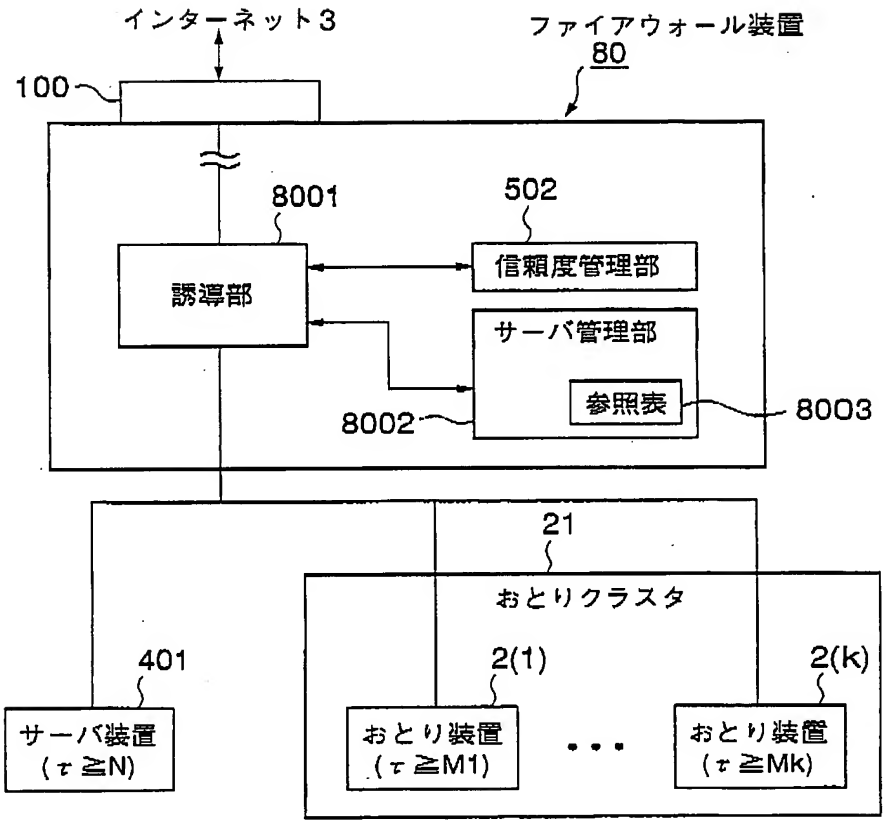


図62

8003 参照表

サーバ識別子	必須信頼度
D1	M1
D2	M2
・・・	・・・
Dk	Mk

図63

入力パケットpの信頼度τ[p]を算出
11
必須信頼度がτ[p]以下のおとり装置を検索する
12
1つ以上のおとり装置が抽出されたか？
13
N
正規のサーバ装置を仮のおとり装置とみなす
14
Y
対応する識別子を誘導部へ返す
15
求められた識別子で指示されたおとり装置へパケットpを転送する
16
パケットpに対するサーバ動作を検査する
17
サーバからのレスポンスをパケットpの発信元に転送する
18

00537

図64

ファイアウォール装置
81
8101
信頼度管理部
8102
アラート変換部
8103
内部ネットワーク
8104
外部ネットワーク
攻撃検知システム
AD1
攻撃検知システム
AD2
攻撃検知システム
AD3
攻撃検知システム
ADN

00537

図65

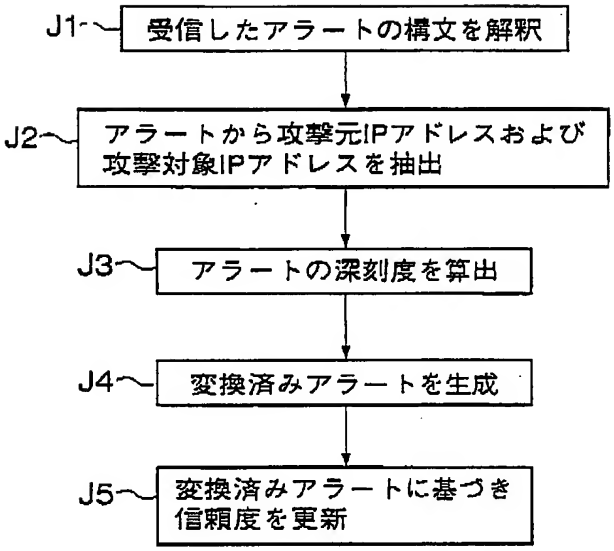
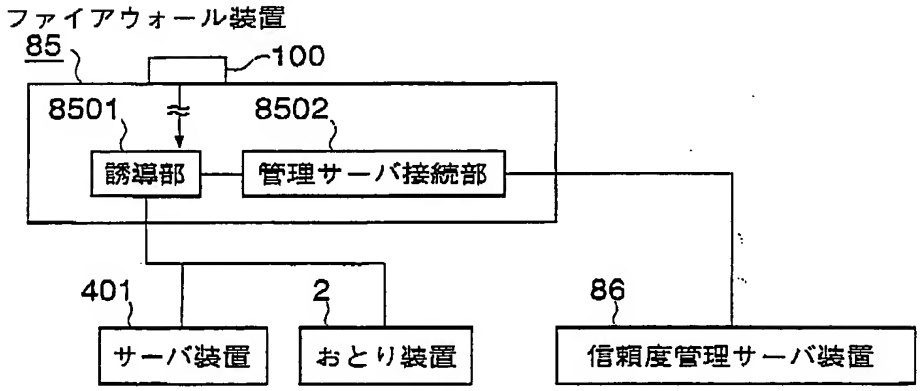


図66



00537

図67

ファイアウォール装置 85
信頼度管理サーバ装置 86
K1
入力パケットpの受信
K2
pに関する信頼度要求メッセージを信頼度管理サーバに送信
K3
信頼度要求メッセージからpを抽出
K4
pに対する信頼度τ[p]を算出
K5
τ[p]を含む応答メッセージを送信
K6
応答メッセージからτ[p]を抽出
K7
τ[p]に基づいて転送先を決定しpを転送する